

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :
Hiroki YAMAUCHI et al. :
Serial No. NEW : Attn: APPLICATION BRANCH
Filed August 28, 2003 : Attorney Docket No. 2003_1212A

CONTENT-DUPLICATION MANAGEMENT:
SYSTEM, APPARATUS AND METHOD,
PLAYBACK APPARATUS AND METHOD, :
AND COMPUTER PROGRAM

THE COMMISSIONER IS AUTHORIZED
TO CHARGE ANY DEFICIENCY IN THE
FEES FOR THIS PAPER TO DEPOSIT
ACCOUNT NO. 23-0975

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

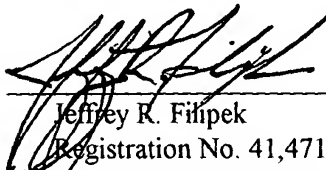
Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2002-249215, filed August 28, 2002, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Hiroki YAMAUCHI et al.

By


Jeffrey R. Filipek
Registration No. 41,471
Attorney for Applicants

JRF/fs
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
August 28, 2003

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 8月28日

出 願 番 号

Application Number:

特願2002-249215

[ST.10/C]:

[JP2002-249215]

出 願 人

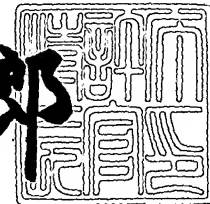
Applicant(s):

松下電器産業株式会社

2003年 5月30日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3040855

【書類名】 特許願

【整理番号】 2022540326

【提出日】 平成14年 8月28日

【あて先】 特許庁長官 殿

【国際特許分類】 G11B 20/10
G09C 1/00
G06F 12/14

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 山内 弘貴

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 太田 雄策

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 宮▲さき▼ 雅也

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 松崎 なつめ

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
会社内

【氏名】 阿部 敏久

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100090446

【弁理士】

【氏名又は名称】 中島 司朗

【手数料の表示】

【予納台帳番号】 014823

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9003742

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報複製管理システムおよび端末

【特許請求の範囲】

【請求項 1】 複数の端末が互いに通信網で接続されたネットワークシステムにおいて、

前記端末は、情報を格納するための記憶部と、他の端末と通信網を介して通信するための通信部と、他端末の正当性を確認するための認証部とを有し、

更に、前記ネットワークシステム内に 1 台以上存在する第 1 の端末は、自らの記憶部または他端末内の記憶部に保管された情報の複製制限情報を管理する複製制限情報管理部を有しており、

前記複製制限情報管理部は、第 2 の端末から通信網を介して第 1 の端末に送付された情報複製要求、または複製情報の返却要求の正当性を認証部で確認した後、当該情報の複製または返却の是非を前記複製制限情報を基に判断し、複製または返却を許可した場合には、当該情報の複製制限情報を保持または更新することを特徴とする情報複製管理システム。

【請求項 2】 前記端末が着脱可能な記憶媒体を使用可能な場合において、

前記着脱可能な記憶媒体は、情報を格納するための媒体内記憶部と、端末との正当性を確認するための媒体内認証部とを有し、

前記端末は、更に着脱可能記憶媒体用入出力部を有し、

前記端末の認証部は、前記媒体内認証部との間で、前記端末および着脱可能な記憶媒体の正当性を確認し、

前記複製制限情報管理部は、第 1 または第 2 の端末に挿入された着脱可能記憶媒体への情報複製要求、または前記着脱可能記憶媒体からの複製情報の返却要求の正当性を認証部で確認した後、当該情報の複製または返却の是非を前記複製制限情報を基に判断し、複製または返却を許可した場合には、当該情報の複製制限情報を保持または更新することを特徴とする請求項 1 記載の情報複製管理システム。

【請求項 3】 前記第 2 の端末が他端末より情報を複製、または多端末へ複製情報の返却するために、通信網上に暗号通信路を設定し、情報の送受信を行う場

合において、

前記端末は、更にセッション鍵を格納しているセッション鍵格納部と、前記セッション鍵で通信情報の暗号化または復号化を行う通信情報暗号化部を有し、

前記認証部は、他端末の正当性を確認するとともに、その処理過程でセッション鍵を共有し、

一方の端末では、前記記憶部内の情報を、前記セッション鍵格納部に格納されたセッション鍵を用いて、前記通信情報暗号化部で暗号化した後に、前記通信部から通信網に送信し、

もう一方の端末では、通信網介して送信されてきた暗号化情報を前記通信部で受信した後に、前記暗号化情報を、前記セッション鍵格納部に格納されたセッション鍵を用いて、前記通信情報暗号化部で復号化し、前記記憶部に格納することを特徴とする請求項 1 および請求項 2 記載の情報複製管理システム。

【請求項 4】 前記第 1 の端末が、前記第 2 の端末の情報複製要求、または複製情報の返却要求を許可し、前記複製制限情報を更新中に、他の端末の情報複製要求、または複製情報の返却要求を許可する場合において、

前記第 1 の端末は、更に前記複製情報管理部に、更新中の複製制限情報を他の処理で更新できないようにするための複製制限情報排他制御部を有し、

前記複製制限情報排他制御部は、更新中の前記複製制限情報が更新を完了した場合に、事前に規定した方法で次の更新処理を順次選択することを特徴とする請求項 1、請求項 2 および請求項 3 記載の情報複製管理システム。

【請求項 5】 前記事前に規定した方法が、更新処理の到着順であることを特徴とする請求項 4 記載の情報複製管理システム。

【請求項 6】 前記事前に規定した方法が、更新処理に設定された優先度順であることを特徴とする請求項 4 記載の情報複製管理システム。

【請求項 7】 前記複製制限情報に情報の複製数を含み、当該情報の複製の是非を前記複製数を加味して判断し、複製を許可した場合には、当該情報の複製数を更新することを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 8】 前記複製制限情報に情報の複製数を含み、複製情報の返却を許

可した場合には、当該情報の複製数を更新することを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 9】 前記複製制限情報に情報のグループ内端末への複製数（グループ内複製数）を含み、当該情報の複製の是非を前記グループ内複製数を加味して判断し、複製を許可した場合には、当該情報のグループ内複製数を更新することを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 10】 前記複製制限情報に情報のグループ内複製数を含み、複製情報の返却を許可した場合には、当該情報のグループ内複製数を更新することを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 11】 前記複製制御情報に情報のグループ外端末への複製数（グループ外複製数）を含み、当該情報の複製の是非を前記グループ外複製数を加味して判断し、複製を許可した場合には、当該情報のグループ外複製数を更新することを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 12】 前記複製制御情報に、情報のグループ外端末への複製の是非を記したグループ外複製可否情報を含み、当該情報の複製の是非を前記グループ外複製可否情報を加味して判断することを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 13】 前記複製制限情報に、情報の着脱可能な記録媒体への複製数（着脱可能記録媒体内複製数）を含み、当該情報の複製の是非を前記着脱可能記録媒体内複製数を加味して判断し、複製を許可した場合には、当該情報の着脱可能記録媒体内複製数を更新することを特徴とする請求項 2 および請求項 3 記載の情報複製管理システム。

【請求項 14】 前記複製制限情報に、情報の着脱可能記録媒体内複製数を含み、複製情報の返却を許可した場合には、当該情報の着脱可能記録媒体内複製数を更新することを特徴とする請求項 2 および請求項 3 記載の情報複製管理システム。

【請求項 1 5】 前記複製制御情報に、情報の現物からの複製回数を記した複製世代情報を含み、当該情報の複製または返却の是非を前記複製世代情報を加味して判断することを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 1 6】 前記複製制御情報に端末のリボケーションリストを含み、当該情報の複製または返却の是非を前記端末のリボケーションリストを加味して判断することを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 1 7】 前記複製制御情報に、複製または返却の可能を指定した時間情報（指定時間情報）を含み、当該情報の複製または返却の是非を前記指定時間情報を加味して判断することを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 1 8】 前記複製制御情報に、複製または返却の可能を指定した地域情報（指定地域情報）を含み、当該情報の複製または返却の是非を前記指定地域情報を加味して判断することを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 1 9】 前記第 2 の端末が複製する情報に、平文情報を含むことを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 2 0】 前記第 2 の端末が複製する情報に、暗号化情報を含むことを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 2 1】 前記第 2 の端末が複製する情報に、暗号化情報を復号するための暗号鍵を含むことを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 2 2】 前記第 2 の端末が複製する情報に、複製制限情報を含むことを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 2 3】 前記第 2 の端末が返却する複製情報に、平文情報を含むこと

を特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 2 4】 前記第 2 の端末が返却する複製情報に、暗号化情報を含むことを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 2 5】 前記第 2 の端末が返却する複製情報に、暗号化情報を復号するための暗号鍵を含むことを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 2 6】 前記第 2 の端末が返却する複製情報に、複製制限情報を含むことを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 2 7】 前記端末は、更に複製した情報の使用可能期間を管理する使用可能期間管理部を有し、

また、前記第 1 の端末は、前記使用可能期間管理部内に複製した情報の使用可能期間が記された使用可能期間情報を有し、

前記第 1 の端末は、前記第 2 の端末からの情報複製要求を許可した場合に、複製制限情報を更新した後に、情報を前記使用可能期間情報とともに配布し、

前記第 2 の端末は、情報の複製時に前記使用可能期間情報を前記使用可能期間管理部に格納し、前記使用可能期間管理部が使用可能期間を終了したことを受けて、情報を消去し、

前記第 1 の端末は、前記複製制限情報を更新することを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 2 8】 前記端末は、更に予め決定した時間に情報の複製または返却を開始する予約処理情報を管理する予約処理管理を有し、

前記第 2 の端末は、複製もしくは返却の指示、およびその開始時間を前記予約処理情報に設定し、前記開始時間の到来を期に、情報の複製もしくは返却を開始し、

前記第 1 の端末は、前記第 2 の端末からの情報複製要求もしくは複製情報の返却要求を許可した場合に、前記複製制限情報を更新することを特徴とする請求項

1、請求項2、請求項3および請求項4記載の情報複製管理システム。

【請求項29】 前記第1の端末は、自らの複製制限情報管理部に保管した情報の複製制限情報を、他の複製制限情報管理部を有した端末に複製し、

前記第2の端末からの情報複製要求または複製情報の返却要求を許可した場合に、自らの複製制限情報管理部に保管した情報の複製制限情報を更新するとともに、他端末に複製した複製制限情報も事前に規定したタイミングで更新することを特徴とする請求項1、請求項2、請求項3および請求項4記載の情報複製管理システム。

【請求項30】 前記事前に規定したタイミングが、第1の端末内の複製制限情報の更新と同時であることを特徴とする請求項29記載の情報複製管理システム。

【請求項31】 前記事前に規定したタイミングが、第1の端末内の複製制限情報の更新後、最も近い一定周期の到来時刻であることを特徴とする請求項29記載の情報複製管理システム。

【請求項32】 前記第1の端末が管理する複製制限情報に関連して、別に設けた課金システムがグループに送付する情報に課金することを特徴とする請求項1、請求項2、請求項3および請求項4記載の情報複製管理システム。

【請求項33】 請求項1から請求項32のいずれか1項に記載の情報複製管理システムにおける端末。

【請求項34】 前記端末の認証部は、許可なく、書き込み、読み出しおよびコピーできない領域に実装することを特徴とする請求項33記載の端末。

【請求項35】 前記端末の複製制限情報管理部は、許可なく、書き込み、読み出しおよびコピーできない領域に実装することを特徴とする請求項33記載の端末。

【請求項36】 請求項2から請求項32のいずれか1項に記載の情報複製管理システムにおける着脱可能な記憶媒体。

【請求項37】 前記情報が複数の端末の記憶部に保管されている場合において、

第2の端末は、更に複製する情報の配布元の端末を決定する情報配布元端末決

定部を有し、

前記情報配布元端末決定部は、事前に規定した方法で複製する情報の配布元の端末を決定することを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム。

【請求項 3 8】 前記事前に規定した方法が、複製する情報を保管している各端末との応答時間を計測し、前記応答時間の最も短い端末を選択することを特徴とする請求項 3 7 記載の情報複製管理システム。

【請求項 3 9】 前記事前に規定した方法が、複製する情報を保管している端末の内、処理性能の最も高い端末を選択することを特徴とする請求項 3 7 記載の情報複製管理システム。

【請求項 4 0】 前記事前に規定した方法が、複製する情報を保管している端末に予め優先度を設定し、前記優先度の最も高い端末を選択することを特徴とする請求項 3 7 記載の情報複製管理システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、例えば、家庭内の端末がネットワークで相互接続され、それらの間ではコンテンツの複製を容易に行え、かつ複製コンテンツの数を規制して著作権の保護を図るコンテンツ複製管理システム、およびそのシステムを構成する端末に関する。

【 0 0 0 2 】

【従来の技術】

近年、映画や音楽などをデジタル化し、蓄積したデジタルコンテンツは、忠実なコピーが可能であるために、著作権保護が困難になってきた。ここで、デジタルコンテンツの著作権保護を行うためのひとつの方策としては、容易な違法コピーを防止することが挙げられる。これを受けて、現在までに、DVD や SD など蓄積メディア用や、HDD プレイヤーなどの AV 機器用コピープロテクション技術が世に出ている。

【 0 0 0 3 】

また、機器メーカーは、A V機器の付加価値を増加させるため、家庭内のA V機器をネットワークで有機的に結び付け、コンテンツの蓄積場所をユーザに意識させず、見たいコンテンツをどこでも視聴できる環境を構築しつつある。

しかし、先に述べたコピープロテクション技術は、著作権者の権利は十分保護されているが、ある機器に保管されたコンテンツを、ユーザの私的利用目的で他の機器へ複製することも容易にできない。そのため、ユーザの利便性が低くなっている。

【0004】

更に、既存のコピープロテクション技術は、機器のネットワークの接続を想定していないため、複数の端末からコンテンツの複製要求を同時に受け付けた場合の対応が不十分である。

【0005】

【発明が解決しようとする課題】

本発明は、著作権者の権利を保護しつつ、ユーザにとって利便性のあるシステムを提供する。具体的には、ユーザの私的利用を目的としたコンテンツの再生／複製等を許可する一方で、その複製数をネットワークを介して明確に制限して著作権者に対する権利の侵害を防止する。

【0006】

【課題を解決するための手段】

本発明の請求項1は、複数の端末が、互いに通信網で接続されたネットワークシステムにおいて、前記端末は、情報を格納するための記憶部と、他の端末と通信網を介して通信するための通信部と、他端末の正当性を確認するための認証部とを有し、更に、前記ネットワークシステム内に1台以上存在する第1の端末は、自らの記憶部または他端末内の記憶部に保管された情報の複製制限情報を管理する複製制限情報管理部を有しており、前記複製制限情報管理部は、第2の端末から通信網を介して第1の端末に送付された情報複製要求、または複製情報の返却要求の正当性を認証部で確認した後に、当該情報の複製または返却の是非を前記複製制限情報を基に判断し、複製または返却を許可した場合には、当該情報の複製制限情報を保持または更新することを特徴とする。

【 0 0 0 7 】

本構成を使用することで、ネットワークに接続された端末間での情報複製および返却を、ユーザの手間を省き、かつ情報の複製制限条件を厳密に満した状態で可能となる。

本発明の請求項 2 は、前記端末が着脱可能な記憶媒体を使用可能な場合において、前記着脱可能な記憶媒体は、情報を格納するための媒体内記憶部と、端末との正当性を確認するための媒体内認証部とを有し、前記端末は、更に着脱可能記憶媒体用入出力部を有し、前記端末の認証部は、前記媒体内認証部との間で、前記端末および着脱可能な記憶媒体の正当性を確認し、前記複製制限情報管理部は、第 1 または第 2 の端末に挿入された着脱可能記憶媒体への情報複製要求、または前記着脱可能記憶媒体からの複製情報の返却要求の正当性を認証部で確認した後、当該情報の複製または返却の是非を前記複製制限情報を基に判断し、複製または返却を許可した場合には、当該情報の複製制限情報を保持または更新することを特徴とする請求項 1 記載の情報複製管理システム

本構成を使用することで、ネットワークに接続された端末および端末に挿入された着脱可能な記憶媒体間での情報複製および返却を、ユーザの手間を省き、かつ情報の複製制限条件を厳密に満した状態で可能となる。

【 0 0 0 8 】

本発明の請求項 3 は、前記第 2 の端末が他端末より情報を複製、または多端末へ複製情報の返却するために、通信網上に暗号通信路を設定し、情報の送受信を行う場合において、前記端末は、更にセッション鍵を格納しているセッション鍵格納部と、前記セッション鍵で通信情報の暗号化または復号化を行う通信情報暗号化部を有し、前記認証部は、他端末の正当性を確認するとともに、その処理過程でセッション鍵を共有し、一方の端末では、前記記憶部内の情報を、前記セッション鍵格納部に格納されたセッション鍵を用いて、前記通信情報暗号化部で暗号化した後に、前記通信部から通信網に送信し、もう一方の端末では、通信網介して送信されてきた暗号化情報を前記通信部で受信した後に、前記暗号化情報を、前記セッション鍵格納部に格納されたセッション鍵を用いて、前記通信情報暗号化部で復号化し、前記記憶部に格納することを特徴とする。

【 0 0 0 9 】

本構成を使用することで、情報の送受信を暗号通信路上で行うことができるようになり、悪意のある第 3 者が当該情報の内容入手することを困難にする。

本発明の請求項 4 は、前記第 1 の端末が、前記第 2 の端末の情報複製要求、または複製情報の返却要求を許可し、前記複製制限情報を更新中に、他の端末の情報複製要求、または複製情報の返却要求を許可する場合において、前記第 1 の端末は、更に前記複製情報管理部に、更新中の複製制限情報を他の処理で更新できないようにするための複製制限情報排他制御部を有し、前記複製制限情報排他制御部は、更新中の前記複製制限情報が更新を完了した場合に、事前に規定した方法で次の更新処理を順次選択することを特徴とする。

【 0 0 1 0 】

本構成を使用することで、複数の端末から行われた複製制限情報の更新処理が、誤りなく順次実行することが可能となる。

本発明の請求項 5 は、請求項 4 に記載した事前に規定した方法が、更新処理の到着順であることを特徴とする。

本構成を使用することで、複数の端末から行われた複製制限情報の更新処理が、誤りなく順次実行することが可能となる。

【 0 0 1 1 】

本発明の請求項 6 は、請求項 4 に記載した事前に規定した方法が、更新処理に設定された優先度順であることを特徴とする。

本構成を使用することで、複数の端末から行われた複製制限情報の更新処理が、誤りなく順次実行することが可能となる。

本発明の請求項 7 は、前記複製制限情報に情報の複製数を含み、当該情報の複製の是非を前記複製数を加味して判断し、複製を許可した場合には、当該情報の複製数を更新することを特徴とする。

【 0 0 1 2 】

本構成を使用することで、ネットワークに接続された端末および端末に挿入された着脱可能な記憶媒体内で、ユーザの手間を省き、かつ情報の複製数を制限された値以下にすることが可能となる。

本発明の請求項 8 は、前記複製制限情報に情報の複製数を含み、複製情報の返却を許可した場合には、当該情報の複製数を更新することを特徴とする。

【 0 0 1 3 】

本構成を使用することで、ネットワークに接続された端末および端末に挿入された着脱可能な記憶媒体内で、ユーザの手間を省き、かつ情報の複製数を制限された値以下にすることが可能となる。

本発明の請求項 9 は、前記複製制限情報に情報のグループ内端末への複製数（グループ内複製数）を含み、当該情報の複製の是非を前記グループ内複製数を加味して判断し、複製を許可した場合には、当該情報のグループ内複製数を更新することを特徴とする。

【 0 0 1 4 】

本構成を使用することで、ネットワークに接続されたグループ内の端末および端末に挿入された着脱可能な記憶媒体内で、ユーザの手間を省き、かつ情報のグループ内端末および着脱可能な記憶媒体への複製数を制限された値以下にすることが可能となる。

本発明の請求項 1 0 は、前記複製制限情報に情報のグループ内複製数を含み、複製情報の返却を許可した場合には、当該情報のグループ内複製数を更新することを特徴とする。

【 0 0 1 5 】

本構成を使用することで、ネットワークに接続されたグループ内の端末および端末に挿入された着脱可能な記憶媒体内で、ユーザの手間を省き、かつ情報のグループ内端末および着脱可能な記憶媒体への複製数を制限された値以下にすることが可能となる。

本発明の請求項 1 1 は、前記複製制御情報に情報のグループ外端末への複製数（グループ外複製数）を含み、当該情報の複製の是非を前記グループ外複製数を加味して判断し、複製を許可した場合には、当該情報のグループ外複製数を更新することを特徴とする。

【 0 0 1 6 】

本構成を使用することで、ネットワークに接続されたグループ外の端末および

グループ外端末に挿入された着脱可能な記憶媒体に対し、ユーザの手間を省き、かつ情報のグループ内端末および着脱可能な記憶媒体への複製数を制限された値以下にすることが可能となる。

本発明の請求項 1 2 は、前記複製制御情報に、情報のグループ外端末への複製の是非を記したグループ外複製可否情報を含み、当該情報の複製の是非を前記グループ外複製可否情報を加味して判断することを特徴とする。

【 0 0 1 7 】

本構成を使用することで、ネットワークに接続されたグループ外の端末および端末に挿入された着脱可能な記憶媒体に対し、ユーザの手間を省き、かつ情報のグループ外端末および着脱可能な記憶媒体への複製を制限することが可能となる。

本発明の請求項 1 3 は、前記複製制限情報に、情報の着脱可能な記録媒体への複製数（着脱可能記録媒体内複製数）を含み、当該情報の複製の是非を前記着脱可能記録媒体内複製数を加味して判断し、複製を許可した場合には、当該情報の着脱可能記録媒体内複製数を更新することを特徴とする。

【 0 0 1 8 】

本構成を使用することで、ネットワークに接続された端末に挿入された着脱可能な記憶媒体に対し、ユーザの手間を省き、かつ情報の着脱可能な記憶媒体への複製数を制限された値以下にすることが可能となる。

本発明の請求項 1 4 は、前記複製制限情報に、情報の着脱可能記録媒体内複製数を含み、複製情報の返却を許可した場合には、当該情報の着脱可能記録媒体内複製数を更新することを特徴とする。

【 0 0 1 9 】

本構成を使用することで、ネットワークに接続された端末に挿入された着脱可能な記憶媒体に対し、ユーザの手間を省き、かつ情報の着脱可能な記憶媒体への複製数を制限された値以下にすることが可能となる。

本発明の請求項 1 5 は、前記複製制御情報に、情報の現物からの複製回数を記した複製世代情報を含み、当該情報の複製または返却の是非を前記複製世代情報を加味して判断することを特徴とする。

【 0 0 2 0 】

本構成を使用することで、前記複製制御情報に複製世代情報含み、ユーザの手間を省き、かつ情報の端末および着脱可能な記憶媒体への複製または返却を複製世代情報を基に制限することが可能となる。

本発明の請求項 1 6 は、前記複製制御情報に端末のリボケーションリストを含み、当該情報の複製または返却の是非を前記端末のリボケーションリストを加味して判断することを特徴とする。

【 0 0 2 1 】

本構成を使用することで、ネットワークに接続された端末に挿入された着脱可能な記憶媒体に対し、ユーザの手間を省き、かつ不正行為のため使用できなくなった端末および着脱可能な記憶媒体への複製または返却を制限することが可能となる。

本発明の請求項 1 7 は、前記複製制御情報に、複製または返却の可能を指定した時間情報（指定時間情報）を含み、当該情報の複製または返却の是非を前記指定時間情報を加味して判断することを特徴とする請求項 1、請求項 2、請求項 3 および請求項 4 記載の情報複製管理システム

本構成を使用することで、ネットワークに接続された端末に挿入された着脱可能な記憶媒体に対し、ユーザの手間を省き、かつ情報の端末および着脱可能な記憶媒体への複製または返却を指定時間情報を基に制限することが可能となる。

【 0 0 2 2 】

本発明の請求項 1 8 は、前記複製制御情報に、複製または返却の可能を指定した地域情報（指定地域情報）を含み、当該情報の複製または返却の是非を前記指定地域情報を加味して判断することを特徴とする。

本構成を使用することで、ネットワークに接続された端末に挿入された着脱可能な記憶媒体に対し、ユーザの手間を省き、かつ情報の端末および着脱可能な記憶媒体への複製または返却を指定時間情報を基に制限することが可能となる。

【 0 0 2 3 】

本発明の請求項 1 9 は、前記第 2 の端末が複製する情報に、平文情報を含むことを特徴とする。

本発明の請求項 2 0 は、前記第 2 の端末が複製する情報に、暗号化情報を含むことを特徴とする。

本発明の請求項 2 1 は、前記第 2 の端末が複製する情報に、暗号化情報を復号するための暗号鍵を含むことを特徴とする。

【 0 0 2 4 】

本発明の請求項 2 2 は、前記第 2 の端末が複製する情報に、複製制限情報を含むことを特徴とする。

本発明の請求項 2 3 は、前記第 2 の端末が返却する複製情報に、平文情報を含むことを特徴とする。

本発明の請求項 2 4 は、前記第 2 の端末が返却する複製情報に、暗号化情報を含むことを特徴とする。

【 0 0 2 5 】

本発明の請求項 2 5 は、前記第 2 の端末が返却する複製情報に、暗号化情報を復号するための暗号鍵を含むことを特徴とする。

本発明の請求項 2 6 は、前記第 2 の端末が返却する複製情報に、複製制限情報を復号するための暗号鍵を含むことを特徴とする。

本発明の請求項 2 7 は、前記端末は、更に複製した情報の使用可能期間を管理する使用可能期間管理部を有し、また、前記第 1 の端末は、前記使用可能期間管理部内に複製した情報の使用可能期間が記された使用可能期間情報を有し、前記第 1 の端末は、前記第 2 の端末からの情報複製要求を許可した場合に、複製制限情報を更新した後に、情報を前記使用可能期間情報とともに配布し、前記第 2 の端末は、情報の複製時に前記使用可能期間情報を前記使用可能期間管理部に格納し、前記使用可能期間管理部が使用可能期間を終了したことを受けて、情報を消去し、前記第 1 の端末は、前記複製制限情報を更新することを特徴とする。

【 0 0 2 6 】

本構成を使用することで、複製した情報を使用可能期間内のみ使用することが可能となり、かつ使用可能期間を経過した場合には、複製情報を無効化し、当該情報の複製制限情報を元に戻すことが可能となる。

本発明の請求項 2 8 は、前記端末は、更に予め決定した時間に情報の複製また

は返却を開始する予約処理情報を管理する予約処理管理を有し、前記第 2 の端末は、複製もしくは返却の指示、およびその開始時間を前記予約処理情報に設定し、前記開始時間の到来を期に、情報の複製もしくは返却を開始し、前記第 1 の端末は、前記第 2 の端末からの情報複製要求もしくは複製情報の返却要求を許可した場合に、前記複製制限情報を更新することを特徴とする。

【 0 0 2 7 】

本構成を使用することで、更に予め決定した時間に情報を複製または返却するため、それに要する時間を待たずに、次の行動をすることが可能となる。

本発明の請求項 2 9 は、前記第 1 の端末は、自らの複製制限情報管理部に保管した情報の複製制限情報を、他の複製制限情報管理部を有した端末に複製し、前記第 2 の端末からの情報複製要求または複製情報の返却要求を許可した場合に、自らの複製制限情報管理部に保管した情報の複製制限情報を更新するとともに、他端末に複製した複製制限情報も事前に規定したタイミングで更新することを特徴とする。

【 0 0 2 8 】

本構成を使用することで、情報の複製制限情報を管理している端末が故障した場合でも、引き続き情報の複製または返却が可能となる。

本発明の請求項 3 0 は、前記事前に規定したタイミングが、第 1 の端末内の複製制限情報の更新と同時であることを特徴する。

本構成を使用することで、情報の複製制限情報を管理している端末が故障した場合でも、引き続き情報の複製または返却が可能となる。

【 0 0 2 9 】

本発明の請求項 3 1 は、前記事前に規定したタイミングが、第 1 の端末内の複製制限情報の更新後、最も近い一定周期の到来時刻であることを特徴する。

本構成を使用することで、情報の複製制限情報を管理している端末が故障した場合でも、引き続き情報の複製または返却が可能となる。

本発明の請求項 3 2 は、前記第 1 の端末が管理する複製制限情報に関連して、別に設けた課金システムがグループに送付する情報に課金することを特徴とする。

【 0 0 3 0 】

本構成を使用することで、情報の複製制限情報に関連して、情報の価格を設定することが可能となる。

本発明の請求項 3 3 は、請求項 1 から請求項 3 2 のいずれか 1 項に記載の情報複製管理システムにおける端末である。

本発明の請求項 3 4 は、前記端末の認証部は、許可なく、書き込み、読み出しおよびコピーできない領域に実装することを特徴とする。

【 0 0 3 1 】

本構成を使用することで、悪意のある第 3 者が前記端末の認証部を不正に改造し、不正に情報を複製することを防ぐ。

本発明の請求項 3 5 は、前記端末の複製制限情報管理部は、許可なく、書き込み、読み出しおよびコピーできない領域に実装することを特徴とする。

本構成を使用することで、悪意のある第 3 者が前記端末の複製制限情報管理部を不正に改造し、不正に情報を複製することを防ぐ。

【 0 0 3 2 】

本発明の請求項 3 6 は、請求項 1 から請求項 3 2 のいずれか 1 項に記載の情報複製管理システムにおける着脱可能な記憶媒体である。

本発明の請求項 3 7 は、前記情報が複数の端末の記憶部に保管されている場合において、第 2 の端末は、更に複製する情報の配布元の端末を決定する情報配布元端末決定部を有し、前記情報配布元端末決定部は、事前に規定した方法で複製する情報の配布元の端末を決定することを特徴とする。

【 0 0 3 3 】

本構成を使用することで、情報の配布元処理がひとつの端末に集中せず、かつ情報を保管した端末が故障した場合でも、その他の端末から情報を入手することが可能となる。

本発明の請求項 3 8 は、前記事前に規定した方法が、複製する情報を保管している各端末との応答時間を計測し、前記応答時間の最も短い端末を選択することを特徴とする。

【 0 0 3 4 】

本構成を使用することで、情報を短時間に入手することが可能となる。

本発明の請求項 3 9 は、前記事前に規定した方法が、複製する情報を保管している端末の内、処理性能の最も高い端末を選択することを特徴とする。

本構成を使用することで、処理能力の余裕がある端末を情報の配布元することができ、配布元端末内の他の処理に影響を少なくすることが可能となる。

【 0 0 3 5 】

本発明の請求項 4 0 は、前記事前に規定した方法が、複製する情報を保管している端末に予め優先度を設定し、前記優先度の最も高い端末を選択することを特徴とする。

本構成を使用することで、予め設定したポリシーを元に、配布元端末を選択することが可能となる。

【 0 0 3 6 】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照しながら詳細に説明する。なお、以下の実施の形態は、本発明を具体化した一例であって、本発明の技術的範囲を限定する性格のものではない。

（実施の形態 1）

本発明の実施の形態 1 に係る情報複製管理システム 1 0 1 を図 1 を用いて説明する。

【 0 0 3 7 】

まず、情報複製管理システム 1 0 1 では、複数のサーバや端末をひと括りとしたグループ 1 0 2 という概念が存在し、そのグループ内では音楽や映像などのデジタルコンテンツを、予め決められた数以下であれば自由に複製することができる。また、複製したコンテンツを複製元に返却することで、一度減少した複製可能数を増加させることもできる。一方、グループ外への複製に関しては、外部への持ち出しという形式を選択することができ、返却はできないものとする。

【 0 0 3 8 】

情報複製管理システム 1 0 1 は、グループ内サーバ 1 0 4、グループ内端末 1 0 5、グループ内端末 2 1 0 6 およびグループ外端末 1 1 0 7 がネット

ワーク 1 0 3 で接続された構成で、グループ内サーバ 1 0 4、グループ内端末 1 0 5 およびグループ内端末 2 1 0 6 は先に説明したグループ 1 0 2 に属している。なお、ネットワーク 1 0 3 の通信プロトコルの一例としては、TCP/IP や、IEEE 1 3 9 4 などが挙げられる。

【0 0 3 9】

ここで、グループ 1 0 2 は、グループ 1 0 2 内のサーバおよび端末で、グループに属していることを証明するグループ所属情報 2 1 1 を共有することで実現している。このグループ証明情報は、秘匿的に各端末に配布された共通秘密情報や、外部の認証機関が発行したグループを構成する機器リストなどである。

このように、グループを定義することで、ユーザの私的利用におけるコンテンツ複製をゆるしつつ、複製の範囲を有限なものとして明確に定義することが可能となり、コンテンツの無制限な複製およびグループ外への流出を防止することができる。

【0 0 4 0】

以下では、次の 3 つのコンテンツ複製または返却の処理フローを詳細に説明する。

- (1) グループ内サーバから、グループ内端末 1 へのコンテンツ複製
- (2) グループ内端末 1 から、グループ内サーバへのコンテンツ返却
- (3) グループ内サーバから、グループ外端末 1 へのコンテンツ複製

下記説明の前提条件として、コンテンツは、

1. 暗号化コンテンツ
2. 暗号化コンテンツを復号化するための暗号鍵

で構成されており、

その複製制限情報としては

1. グループ内複製数：M (M は整数で、グループ内で複製可能な数を表す)
2. グループ外複製数：N (N は整数で、グループ内で複製可能な数を表す)

3. グループ外複製可否情報: YES/NO (YESの場合にはグループ外への複製を許可し、NOの場合にはグループ外への複製を禁止する) を持つものとする。

<<(1) グループ内サーバから、グループ内端末1へのコンテンツ複製>>

図2に、グループ内サーバ104、グループ内端末1 105およびグループ内端末2の内部構成と、各機器間のネットワーク接続形態を示す。なお、図2では本発明を特徴付ける構成要素のみを記載しており、グループ端末2の内部構造はグループ端末1の内部構造と等しいため省略している。

【0041】

グループ内サーバ104および端末105、106の内部としては、コンテンツを記憶しておくための記憶部201、221と、コンテンツの複製を要求した端末が不正な機器でないことの判断と、グループに属しているかを判断し、暗号通信用のセッション鍵を生成する認証部202、222と、機器間の通信を制御する通信部203、223と、セッション鍵を格納するセッション鍵格納部205、225と、通信する情報を暗号化する通信情報暗号部206、226で構成されている。

【0042】

更に、グループ内サーバには、記憶部201に保管されたコンテンツの複製制限情報221(グループ内複製数、グループ外複製数、グループ外複製可否情報)を格納する複製制限情報管理部204を有する。なお、複製制限情報管理部204内には、複数端末、例えばグループ内端末1 105とグループ内端末2 106から同時期にコンテンツ複製要求がなされた場合に、複製制限情報212へのアクセス競合による問題を解決するために、複製制限情報排他制御部207が格納されている。ここで、本実施の形態では複製制限情報排他制御部207内に、キューを設け、処理要求が到着した順番に複製制限情報212をアクセス可能にする。

【0043】

なお、本実施例では複製制限情報管理部204をグループ内サーバ104にの

み実装しているが、全ての端末にも実装しても構わない。

また、認証部202、222や複製制限情報管理部204は、不正なコンテンツ複製を防止するための重要な情報が格納されているため、ハッカーによる不正改造を防ぐため、耐タンパ構造で実装しても構わない。

【0044】

以下、図3のフローチャートを用いて、グループ内端末1 105からグループ内サーバ104へ、コンテンツの複製要求を行った場合の手順を説明する。

最初に、グループ内端末1 105の利用者は、通信部223を用いてグループ内サーバ104に複製要求を送信する（ステップS300）。

グループ内サーバ104は、自身の通信部203により複製要求を受信すると、認証部202は、通信部203、223を介し、グループ内端末1 105の認証部222との間で、認証処理を行う（ステップS301）。

【0045】

認証処理の結果、グループ内端末1 105が不正な機器でないこと確認する（ステップS302）。もし、グループ外端末1 107が不正な機器と確認された場合には、本複製要求を棄却し、その旨をグループ内サーバ104からグループ内端末1 105へ通知し（ステップS303）、一連の処理を終了する。一方、グループ外端末1 107が不正な機器でないと確認された場合には、更にグループ所属情報211を所有していることを確認する（ステップS304）。もし、同一グループであることが確認されると暗号通信用のセッション鍵生成を行う（ステップS305）。そして、生成されたセッション鍵213、232をそれぞれのセッション鍵格納部205、225に格納する（ステップ306）。ここで、上記の認証処理と暗号通信用のセッション鍵213、232の生成は、例えばDTCP (Digital Transmission Content Protection) で採用しているAKE (Authentication and Key Exchange) と同様な方法を利用する。

【0046】

一方、グループ内端末1 105がグループ外の機器であると確認された場合には、グループ外端末用処理に移る。

次に、グループ内サーバ104は、グループ内端末1105が自分と同じグループに属していることを確認した場合には、複製制限情報管理部204内の複製制限情報を更新するに当たり、その処理要求を複製制限情報排他制御部207内のキューの最後尾に挿入する（ステップS307）。この後、継続的に当該処理要求がキューの先頭にきたかを確認する（ステップS308）。

もし、当該処理要求がキューの先頭の場合には、複製制限情報のグループ内複製数が「0」でないことを確認し（ステップS309）、もし「0」以外の場合にはコンテンツを通信情報暗号部206へ転送し、セッション鍵で暗号化する（ステップS310）。一方、グループ内複製数が「0」である場合には、本複製要求を棄却し、その旨をグループ内サーバ104からグループ内端末1105へ通知し（ステップS311）、一連の処理を終了する。

ステップS309で暗号化したコンテンツは通信部203を経て、グループ内端末1105の通信部223で受信される（ステップS312）。グループ内端末1105では、受信した暗号化コンテンツを通信情報暗号部206へ転送して復号化する（ステップS313）。そして、復号化したコンテンツを記憶部221に保管し（ステップS314）、グループ内サーバ104へコンテンツの受信完了を通知する（ステップS315）。グループ内サーバ104は、グループ内端末1105からの受信完了通知を受信すると、現状のグループ内複製数から「1」を差し引く（ステップS316）。そして最後に、複製制限情報排他制御部207内のキューより先頭の処理要求を取り除く（ステップS317）。以上で一連の処理が終了する。

<<（2）グループ内端末1から、グループ内サーバへのコンテンツ返却>>

本処理を説明するための端末構成およびその内部構成は、本実施の形態の（1）と同様のため割愛する。ここで、コンテンツの返却時と複製時との大きな差異は、コンテンツをグループ内端末1105から、グループ内サーバ104に転送する必要がないことである。

【0047】

この点を加味し、以下、図4のフローチャートを用いて、グループ内端末1

1 0 5 からグループ内サーバ 1 0 4 へ、コンテンツの返却要求を行った場合の手順を説明する。

最初に、グループ内端末 1 1 0 5 の利用者は、通信部 2 2 3 を用いてグループ内サーバ 1 0 4 に複製返却を送信する（ステップ S 4 0 0）。

【 0 0 4 8 】

グループ内サーバ 1 0 4 は、自身の通信部 2 0 3 により返却要求を受信すると、認証部 2 0 2 は、通信部 2 0 3、2 2 3 を介し、グループ内端末 1 1 0 5 の認証部 2 2 2 との間で、認証処理を行う（ステップ S 4 0 1）。

認証処理の結果、グループ内端末 1 1 0 5 が不正な機器でないこと確認する（ステップ S 4 0 2）。もし、グループ内端末 1 1 0 5 が不正な機器と確認された場合には、本複製要求を棄却し、その旨をグループ内サーバ 1 0 4 からグループ内端末 1 1 0 5 へ通知し（ステップ S 4 0 3）、一連の処理を終了する。一方、グループ内端末 1 1 0 5 が不正な機器でないこと確認された場合には、更にグループ所属情報 2 1 2 を所有していることを確認する（ステップ S 4 0 4）。それに加えて、グループ内端末 1 1 0 5 が本当にコンテンツを保有しているかも確認する。ここで、上記の認証処理は、例えば D T C P (Digital Transmission Content Protection) で採用している A K E (Authentication and Key Exchange) と同様な方法を利用する。

【 0 0 4 9 】

もし、グループ内端末 1 1 0 5 がグループ外の機器であると確認された場合には、その旨をグループ内サーバ 1 0 4 からグループ内端末 1 1 0 5 へ通知し（ステップ S 4 0 5）、一連の処理を終了する。

次に、グループ内サーバ 1 0 4 は、グループ内端末 1 1 0 5 が自分と同じグループに属していることを確認した場合には、複製制限情報管理部 2 0 4 内の複製制限情報 2 1 2 を更新するに当たり、その処理要求を複製制限情報排他制御部 2 0 7 内のキューの最後尾に挿入する（ステップ S 4 0 6）。この後、継続的に当該処理要求がキューの先頭に來たかを確認する（ステップ S 4 0 7）。

【 0 0 5 0 】

もし、当該処理要求がキューの先頭の場合には、その旨をグループ内サーバ 1 0 4 からグループ内端末 1 1 0 5 へ通知する（ステップ S 4 0 8）。

グループ内端末 1 1 0 5 は、記憶部 2 2 1 に保管してあるコンテンツを削除し（ステップ S 4 0 9）、グループ内サーバ 1 0 4 へコンテンツの消去完了を通知する（ステップ S 4 1 0）。グループ内サーバ 1 0 4 は、グループ内端末 1 1 0 5 からの消去完了通知を受信すると、現状のグループ内複製数に「1」を加える（ステップ S 4 1 1）。そして最後に、複製制限情報排他制御部 2 0 7 内のキューより先頭の処理要求を取り除く（ステップ S 4 1 2）。以上で一連の処理が終了する。

<<（3）グループ内サーバから、グループ外端末 1 へのコンテンツ複製>>

図 5 に、グループ内サーバ 1 0 4、グループ外端末 1 1 0 7 の内部構成と、各機器間のネットワーク接続形態を示す。なお、図 5 では本発明を特徴付ける構成要素のみを記載している。

【0051】

ここで、図 5 の内容は、先に説明した図 2 の内容と重複する部分があるため、以下では差異についてのみ説明する。

グループ外端末 1 0 7 の内部としては、コンテンツを記憶しておくための記憶部 5 0 1 と、コンテンツの複製を要求した端末が不正な機器でないことの判断と、暗号通信用のセッション鍵 5 1 1 を生成する認証部 5 0 2 と、機器間の通信を制御する通信部 5 0 3 と、セッション鍵 5 1 1 を格納するセッション鍵格納部 5 0 5 と、通信する情報を暗号化する通信情報暗号部 5 0 6 で構成されている。ここで、グループ外端末 1 1 0 7 はグループ外の機器であるため、その認証部 5 0 2 には、グループ所属情報が存在しない。

【0052】

以下、図 3、図 6 のフローチャートを用いて、グループ外端末 1 1 0 7 からグループ外サーバ 1 0 4 へ、コンテンツの複製要求を行った場合の手順を説明する。ここで、図 6 のフローチャートは、図 3 内のグループ外端末用処理サブルーチン S R 3 0 1 の処理フローである。

最初に、グループ外端末1 107の利用者は、通信部503を用いてグループ内サーバ104に複製要求を送信する（ステップS300）。

【0053】

グループ内サーバ104は、自身の通信部203により複製要求を受信すると、認証部202は、通信部203、503を介し、グループ外端末1 107の認証部502との間で、認証処理を行う（ステップS301）。

認証処理の結果、グループ外端末1 107が不正な機器でないこと確認する（ステップS302）。もし、グループ外端末1 107が不正な機器と確認された場合には、本複製要求を棄却し、その旨をグループ内サーバ104からグループ外端末1 107へ通知し（ステップS303）、一連の処理を終了する。一方、グループ外端末1 107が不正な機器でないと確認された場合には、更にグループ所属情報211を所有していることを確認する（ステップS304）。しかし、グループ外端末1 107は、グループ内サーバ104と同じグループに属していないため、グループ外機器と確認され、グループ外端末用処理に移る。

【0054】

グループ外端末用処理では、まずグループ内サーバ104は、グループ外端末1 107が複製を要求しているコンテンツの複製制限情報のグループ外複製可否情報を確認する（ステップS600）。もし、グループ外複製可否情報がNOの場合には、本複製要求を棄却し、その旨をグループ内サーバ104からグループ外端末1 107へ通知し（ステップS601）、一連の処理を終了する。一方、グループ外複製可否情報がYESの場合には、暗号通信用のセッション鍵生成を行う（ステップS602）。そして、生成されたセッション鍵をそれぞれのセッション鍵格納部205、505に格納する（ステップ603）。ここで、上記の認証処理と暗号通信用のセッション鍵の生成は、例えばDTCP（Digital Transmission Content Protection）で採用しているAKE（Authentication and Key Exchange）と同様な方法を利用する。

【0055】

次に、グループ内サーバ104は、複製制限情報管理部204内の複製制限情報を更新するに当たり、その処理要求を複製制限情報排他制御部207内のキューの最後尾に挿入する（ステップS604）。この後、継続的に当該処理要求がキューの先頭にきたかを確認する（ステップS605）。

もし、当該処理要求がキューの先頭の場合には、複製制限情報のグループ外複製数が「0」でないことを確認し（ステップS606）、もし「0」以外の場合にはコンテンツを通信情報暗号部206へ転送し、セッション鍵で暗号化する（ステップS607）。一方、グループ外複製数が「0」である場合には、本複製要求を棄却し、その旨をグループ内サーバ104からグループ外端末1107へ通知し（ステップS608）、一連の処理を終了する。

【0056】

（ステップS607）で暗号化したコンテンツは通信部203を経て、グループ外端末1107の通信部223で受信される（ステップS608）。グループ外端末1107では、受信した暗号化コンテンツを通信情報暗号部506へ転送して復号化する（ステップS609）。そして、復号化したコンテンツを記憶部501に保管し（ステップS610）、グループ内サーバ104へコンテンツの受信完了を通知する（ステップS611）。グループ内サーバ104は、グループ外端末1107からの受信完了通知を受信すると、現状のグループ外複製数から「1」を差し引く（ステップS612）。そして最後に、複製制限情報排他制御部207内のキューより先頭の処理要求を取り除く（ステップS317）。以上で一連の処理が終了する。

上記のように本発明の第1の実施の形態では、認証部を有するサーバおよび端末をネットワークで接続することにより、グループ内外の区別が可能となり、複製の範囲を有限なものにとどめる事で、情報の不正な複製の拡大を防止できる。

【0057】

また、グループ内におけるユーザの私的利用を目的とした複製に関しても、これまでのコピープロテクション技術に比べ自由度が高く、ユーザの利便性を高めることができる。

更に、ネットワークに接続される複数の端末から同時にコンテンツの複製要求がきた場合でも、複製制限情報の更新処理が誤りなく順次実行することができる。

【 0 0 5 8 】

以上に加えて、コンテンツをネットワーク上に転送する際に、暗号通信路を使用するため、悪意のある第 3 者がコンテンツの内容を入手することを困難にできる。

なお、以上の説明では、複製制限情報としてグループ内複製数、グループ外複製およびグループ外複製可否情報のみを使用した。が、情報の現物からの複製回数を記した複製世代情報や、端末のリボケーションリスト、複製の可能を指定した時間情報（指定時間情報）、複製または返却の可能を指定した地域情報（指定地域情報）なども考慮に入れて、複製の可否を決定しても構わない。

【 0 0 5 9 】

また、複製するコンテンツとして、暗号化コンテンツと、暗号化コンテンツを復号化するための暗号鍵の組み合わせを用いたが、暗号化コンテンツや暗号化コンテンツを復号化するための暗号鍵、平文のコンテンツ、複製制限情報の様々な組み合わせをコンテンツとしても構わない。

また、以上の説明では、グループ内複製数とグループ外複製数を独立に管理したが、その合計でコンテンツを複製できる個数の上限を管理しても構わない。

【 0 0 6 0 】

また、コンテンツ毎にグループ内サーバを決定しても構わない。

また、本システムは、コンテンツの配布時に複製制限情報の内容に応じて課金するシステムと一緒に使用しても構わない。

（実施の形態 2）

本発明の実施の形態 2 に係る情報複製管理システム 7 0 1 を図 7 を用いて説明する。

【 0 0 6 1 】

まず、情報複製管理システム 7 0 1 の場合も、実施の形態 1 で説明したグルー

プ 102 の概念が同様に存在するものとする。

情報複製管理システム 701 は、グループ内サーバ 104、グループ内端末 105、グループ外端末 107、グループ内着脱可能記憶媒体 1702、グループ内着脱可能記憶媒体 2703 およびグループ外着脱可能記憶媒体 1704 が、ネットワーク 103 で接続された構成で、グループ内サーバ 104 とグループ内端末 105、グループ内着脱可能記憶媒体 2703 およびグループ外着脱可能記憶媒体 1704 はグループ 102 を形成している。

【0062】

以下では、次の 4 つのコンテンツ複製または返却の処理フローを詳細に説明する。

(1) グループ内サーバから、そのサーバに接続されたグループ内着脱可能記憶媒体へのコンテンツ複製

(2) グループ内サーバに接続されたグループ内着脱可能記憶媒体から、そのサーバへのコンテンツ返却

(3) グループ内サーバから、グループ内端末 1 に接続されたグループ内着脱可能記憶媒体へのコンテンツ複製

(4) グループ内端末 1 に接続されたグループ内着脱可能記憶媒体から、グループ内サーバへのコンテンツ返却

下記説明の前提条件として、コンテンツは、

1. 暗号化コンテンツ

2. 暗号化コンテンツを復号化するための暗号鍵

で構成されており、

その複製制限情報としては

1. グループ内複製数：M (M は整数で、グループ内で複製可能な数を表す)

2. 着脱可能記憶媒体内複製数：K (K は整数で、着脱可能記憶媒体に複製可能な数を表す)

3. グループ外複製可否情報：NO (グループ外への複製を禁止)

を持つものとする。

<< (1) グループ内サーバから、そのサーバに接続されたグループ内着脱可能記憶媒体へのコンテンツ複製 >>

図 8 に、グループ内サーバ 1 0 4、グループ内着脱可能記憶媒体 1 7 0 2 の内部構成と、それら 2 つの接続形態を示す。なお、図 8 では本発明を特徴付ける構成要素のみを記載している。

【 0 0 6 3 】

まず、グループ内サーバ 1 0 4 の内部構成は、新たに着脱可能記憶媒体用入出力部 8 2 0 が追加されたこと以外は、実施の形態 1 で説明したものから変更はない。

次に、グループ内着脱可能記憶媒体 1 7 0 2 の内部構造は、コンテンツを記憶しておくための媒体内記憶部 8 0 1 と、コンテンツの複製を要求した端末が不正な機器でないことの判断と、グループに属しているかを判断する媒体内認証部 8 0 1 で構成されている。

【 0 0 6 4 】

なお、媒体内認証部 8 0 1 は、不正なコンテンツ複製を防止するための重要な情報が格納されているため、ハッカーによる不正改造を防ぐため、耐タンパ構造で実装しても構わない。

以下、図 9 のフローチャートを用いて、グループ内サーバから、そのサーバに接続されたグループ内着脱可能記憶媒体 1 へのコンテンツ複製要求を行った場合の手順を説明する。

【 0 0 6 5 】

最初に、グループ内着脱可能記憶媒体 1 7 0 2 の利用者は、グループ内サーバ 1 0 4 で複製要求を発行する（ステップ S 9 0 0）。

それを受けて、グループ内サーバ 1 0 4 の認証部 2 0 2 は、グループ内着脱可能記憶媒体 1 7 0 2 の媒体認証部 8 0 2 との間で、認証処理を行う（ステップ S 9 0 1）。

【 0 0 6 6 】

認証処理の結果、グループ内着脱可能記憶媒体1 702が不正なメディアでないことを確認する（ステップS902）。もし、グループ内着脱可能記憶媒体1 702が不正なメディアと確認された場合には、本複製要求を棄却し、一連の処理を終了する。

一方、グループ内着脱可能記憶媒体1 702が不正なメディアでないことを確認された場合には、更にグループ所属情報810を所有していることを確認する（ステップS903）。もし、グループ内着脱可能記憶媒体1 702がグループ外のメディアであると確認された場合には、本複製要求を棄却し、一連の処理を終了する。

【0067】

一方、グループ内サーバ104は、グループ内着脱可能記憶媒体1 702が自分と同じグループに属していることを確認した場合には、複製制限情報管理部204内の複製制限情報を更新するに当たり、その処理要求を複製制限情報排他制御部207内のキューの最後尾に挿入する（ステップS904）。この後、継続的に当該処理要求がキューの先頭に来たかを確認する（ステップS905）。もし、当該処理要求がキューの先頭の場合には、複製制限情報のグループ内複製数が「0」でないことを確認し（ステップS906）、もし「0」の場合には本複製要求を棄却し、一連の処理を終了する。一方、「0」以外の場合には、更に、複製制限情報の着脱可能記憶媒体内複製数が「0」でないことを確認し（ステップS907）、もし「0」の場合には本複製要求を棄却し、一連の処理を終了する。一方、「0」以外の場合には、グループ内サーバ104は、記憶部201に格納されているコンテンツ210を、着脱可能記憶媒体用入出力部820を介して、グループ内着脱可能記憶媒体1 702の媒体内記憶部801に書き込む（ステップS908）。グループ内サーバ104は、グループ内着脱可能記憶媒体1 702からの書き込み完了通知を受信すると、現状のグループ内複製数および着脱可能記憶媒体内複製数から「1」を差し引く（ステップS909）。そして最後に、複製制限情報排他制御部207内のキューより先頭の処理要求を取り除く（ステップS910）。以上で一連の処理が終了する。

<< (2) グループ内サーバに接続されたグループ内着脱可能記憶媒体から、そのサーバへのコンテンツ返却 >>

本処理を説明するための端末構成およびその内部構成は、本実施の形態の (1) と同様のため割愛する。ここで、コンテンツの返却時と複製時との大きな差異は、コンテンツをグループ内着脱可能記憶媒体 1 7 0 2 から、グループ内サーバ 1 0 4 に書き戻しする必要がないことである。

【 0 0 6 8 】

この点を加味し、以下、図 1 0 のフローチャートを用いて、グループ内着脱可能記憶媒体 1 7 0 2 からグループ内サーバ 1 0 4 へ、コンテンツの返却要求を行った場合の手順を説明する。

最初に、グループ内着脱可能記憶媒体 1 7 0 2 の利用者は、グループ内サーバ 1 0 4 で返却要求を発行する (ステップ S 1 0 0 0)。

【 0 0 6 9 】

それを受けて、グループ内サーバ 1 0 4 の認証部 2 0 2 は、グループ内着脱可能記憶媒体 1 7 0 2 の媒体認証部 8 0 2 との間で、認証処理を行う (ステップ S 1 0 0 1)。

認証処理の結果、グループ内着脱可能記憶媒体 1 7 0 2 が不正なメディアでないことを確認する (ステップ S 1 0 0 2)。もし、グループ内着脱可能記憶媒体 1 7 0 2 が不正なメディアと確認された場合には、本返却要求を棄却し、一連の処理を終了する。もし、グループ内着脱可能記憶媒体 1 7 0 2 が不正なメディアでないことを確認された場合には、更にグループ所属情報 8 1 0 を所有していることを確認する (ステップ S 1 0 0 3)。もし、グループ内着脱可能記憶媒体 1 7 0 2 がグループ外の機器であると確認された場合には、本返却要求を棄却し、一連の処理を終了する。

【 0 0 7 0 】

一方、グループ内サーバ 1 0 4 は、グループ内着脱可能記憶媒体 1 7 0 2 が自分と同じグループに属していることを確認した場合には、複製制限情報管理部 2 0 4 内の複製制限情報 2 1 2 を更新するに当たり、その処理要求を複製制限情報排他制御部 2 0 7 内のキューの最後尾に挿入する (ステップ S 1 0 0 4)。こ

の後、継続的に当該処理要求がキューの先頭に来たかを確認する（ステップ S 1 0 0 5）。

【 0 0 7 1 】

もし、当該処理要求がキューの先頭の場合には、グループ内サーバ 1 0 4 が媒体内記憶部 8 0 1 に保管してあるコンテンツを削除する（ステップ S 1 0 0 6）。グループ内サーバ 1 0 4 は、グループ内着脱可能記憶媒体 1 7 0 2 からの消去完了通知を受信すると、現状のグループ内複製数および着脱可能記憶媒体内複製数に「1」を加える（ステップ S 1 0 0 7）。そして最後に、複製制限情報排除制御部 2 0 7 内のキューより先頭の処理要求を取り除く（ステップ S 1 0 0 8）。以上で一連の処理が終了する。

<<（3）グループ内サーバから、グループ内端末 1 に接続されたグループ内着脱可能記憶媒体へのコンテンツ複製>>

図 1 1 に、グループ内サーバ 1 0 4、グループ内端末 1 1 0 5、グループ内着脱可能記憶媒体 2 7 0 3 の内部構成と、それらの接続形態を示す。なお、図 1 1 では本発明を特徴付ける構成要素のみを記載している。

【 0 0 7 2 】

なお、本図は、グループ内端末 1 の内部構成に、新たに着脱可能記憶媒体用入出力部 1 1 2 0 が追加されたこと以外は、実施の形態 1 および実施の形態 2 の（1）で説明したものから変更はない。

以下、図 1 2 のフローチャートを用いて、グループ内端末 1 に接続されたグループ内着脱可能記憶媒体 2 から、グループ内サーバへのコンテンツ複製要求を行った場合の手順を説明する。

【 0 0 7 3 】

最初に、グループ内着脱可能記憶媒体 2 7 0 3 の利用者は、グループ内端末 1 1 0 5 で複製要求を発行する（ステップ S 1 2 0 0）。

それを受けて、まずグループ内端末 1 1 0 5 の認証部 2 2 2 は、グループ内着脱可能記憶媒体 2 7 0 3 の媒体認証部 1 1 0 1 との間で、認証処理を行う（ステップ S 1 2 0 1）。

【0074】

認証処理の結果、グループ内着脱可能記憶媒体2 703が不正なメディアでないことを確認する（ステップS1202）。もし、グループ内着脱可能記憶媒体1 702が不正なメディアと確認された場合には、本複製要求を棄却し、一連の処理を終了する。

一方、グループ内着脱可能記憶媒体2 703が不正なメディアでないことを確認された場合には、更にグループ所属情報11110を所有していることを確認する（ステップS1203）。もし、グループ内着脱可能記憶媒体2 703がグループ外のメディアであると確認された場合には、本複製要求を棄却し、一連の処理を終了する。

【0075】

一方、グループ内端末1 105は、グループ内着脱可能記憶媒体1 702が自分と同じグループに属していることを確認した場合には、実施の形態1の（1）で説明した方法で、グループ内サーバ104とグループ内端末1 105間で認証を行い、もし認証が成功した場合、グループ内サーバ104からグループ内端末1 105にコンテンツをダウンロードした後、グループ内複製数および着脱可能記憶媒体内複製数から「1」を差し引く（SR1200）。

【0076】

そして、グループ内端末1 105の記憶部221に一時保管されたコンテンツを、着脱可能記憶媒体用入出力部1120を介して、グループ内着脱可能記憶媒体2 703の媒体内記憶部1101に書き込む（ステップS1204）。最後に、グループ内端末1 105は、記憶部221に一時保管していたコンテンツを消去する（ステップS1205）。以上で一連の処理が終了する。

【0077】

なお、上記の実施の形態では、着脱可能な記憶媒体に格納するコンテンツを、一旦グループ内端末の記憶部に保管したが、サーバから転送されてきたコンテンツを着脱可能な記憶媒体の記憶部に直接書き込んでも構わない。

<<（4）グループ内端末1に接続されたグループ内着脱可能記憶媒体2から、

グループ内サーバへのコンテンツ返却>>

本処理を説明するための端末構成およびその内部構成は、本実施の形態の（３）と同様のため割愛する。

【 0 0 7 8 】

以下、グループ内着脱可能記憶媒体 2 7 0 3 からグループ内サーバ 1 0 4 へ、コンテンツの返却要求を行った場合の手順を説明する。

最初に、本実施の形態の（３）と同様に、まずグループ内端末 1 1 0 5 とグループ内着脱可能記憶媒体 2 7 0 3 間で認証を行う。

次に、実施の形態 1 の（２）で説明した類似の方法で、グループ内サーバ 1 0 4 とグループ内端末 1 1 0 5 間で認証を行い、もし認証が成功した場合、グループ内端末 1 1 0 5 がグループ内着脱可能記憶媒体 2 7 0 3 の媒体内記憶部 1 1 0 1 に保管されているコンテンツを消去し、グループ内複製数および着脱可能記憶媒体内複製数に「１」を加える。以上で一連の処理が終了する。

上記のように本発明の第 2 の実施の形態では、認証部を有するサーバおよび端末をネットワークで接続し、更に認証部を有した着脱可能な記憶媒体をサーバおよび端末で使用可能にすることにより、グループ内外の区別が可能となり、複製の範囲を有限なものにとどめる事で、情報の不正な複製の拡大を防止できる。

【 0 0 7 9 】

また、グループ内におけるユーザの私的利用を目的とした複製に関しても、これまでのコピープロテクション技術に比べ自由度が高く、ユーザの利便性を高めることができる。

また、グループに属した着脱可能な記録媒体にコンテンツを複製できることにより、記録媒体を用いたコンテンツの機器間移動や、機器の故障によるコンテンツの消失防止が可能となる。

【 0 0 8 0 】

更に、ネットワークに接続される複数の端末から同時にコンテンツの複製要求がきた場合でも、複製制限情報の更新処理が誤りなく順次実行することができる。

以上に加えて、着脱可能記憶媒体への複製数を管理しているため、その上限をグループ内複製数より小さい値に設定することで、全て使用可能コンテンツが着脱可能記憶媒体へ流出することが防止できる。

【 0 0 8 1 】

なお、以上の説明では、複製制限情報としてグループ内複製数、着脱可能記憶媒体内複製数およびグループ外複製可否情報のみを使用した。グループ外複製数、情報の現物からの複製回数を記した複製世代情報や、端末のリボケーションリスト、複製の可能を指定した時間情報（指定時間情報）、複製または返却の可能を指定した地域情報（指定地域情報）なども考慮に入れて、複製の可否を決定しても構わない。

【 0 0 8 2 】

また、以上の説明では、グループ内複製数と着脱可能記憶媒体内複製数を独立に管理したが、その合計でコンテンツを複製できる個数の上限を管理しても構わない。

また、複製するコンテンツとして、暗号化コンテンツと、暗号化コンテンツを復号化するための暗号鍵の組み合わせを用いたが、暗号化コンテンツや暗号化コンテンツを復号化するための暗号鍵、平文のコンテンツ、複製制限情報の様々な組み合わせをコンテンツとしても構わない。

（実施の形態 3）

本発明の実施の形態 3 に係る情報複製管理システムを図 1 3 を用いて説明する。

【 0 0 8 3 】

本情報複製管理システムの場合も、実施の形態 1 で説明したグループ 1 0 2 の概念が同様に存在するものとする。

情報複製管理システムは、グループ内サーバ 1 0 4、グループ内端末 1 1 0 5、グループ内端末 2 1 0 6 が、ネットワーク 1 0 3 で接続された構成である。

【 0 0 8 4 】

ここで、本実施の形態の端末には、新たにコンテンツ配布元決定部 1 3 0 3、1 3 3 0 を追加し、暗号化されたコンテンツをどの端末から配布してもらうかを決定する。

まず、本実施の形態の背景としては、暗号化コンテンツは、データ量が通常、暗号鍵のデータ量に比べ十分大きく、通信速度の遅いネットワークを使用した場合には、ダウンロードに長い時間を必要とする。

そのため、本実施の形態では、暗号化コンテンツはグループ内で、自由に配布できるものとし、暗号化コンテンツが既にグループ内サーバ 1 0 4 や、複数のグループ内端末にダウンロードされているものとする。そして、ユーザが実際にその暗号化コンテンツを使用する場合に、グループ内サーバ 1 0 4 へコンテンツの暗号化を解くための暗号鍵を入手するものとする。このようにすることで、実際に使用可能な複製コンテンツの数を制限することが可能となる。

【 0 0 8 5 】

以下、図 1 4 に示すフローチャートを用いて、グループ内端末 1 1 0 5 が暗号鍵と暗号化コンテンツの複製要求を行った場合の手順を説明する。

最初に、グループ内端末 1 1 0 5 は、実施の形態 1 の (1) と同様の方法で、グループ内サーバ 1 0 4 から暗号鍵のみをダウンロードする。それに伴い、グループ内サーバ 1 0 4 は、グループ内複製数から「 1 」だけ差し引く (S R 1 4 0 0) 。

【 0 0 8 6 】

次に、暗号化コンテンツをダウンロードするため、グループ内端末 1 1 0 5 は、まず自端末内の記憶部に暗号化コンテンツが存在するかを確認する (ステップ S 1 4 0 0) 。もし、暗号化コンテンツが自端末内に存在する場合には、一連の処理を終了する。

一方、暗号化コンテンツが自端末内に存在しない場合には、コンテンツ配布元決定部 1 3 0 3 はグループに属している全ての端末に対し、所望の暗号化コンテンツを持っているかを確認する同報通信を通信部 2 2 3 を介して行う (ステップ S 1 4 0 1) 。

【 0 0 8 7 】

その後、コンテンツ配布元決定部 1 3 0 3 は、最も早く応答した暗号化コンテンツを持っている端末を特定する（ステップ S 1 4 0 2）。

そして、特定した端末に対し、実施の形態 1 の（１）と同様の認証処理を実行する（ステップ S 3 0 1 ～ S 3 0 4 および S R 3 0 1）。もし、認証が成功した場合には、暗号化コンテンツを特定した端末よりダウンロードする（ステップ S 1 4 0 3）。最後に、記録部 2 2 1 にダウンロードした暗号化コンテンツを格納する（ステップ S 1 4 0 4）。以上で一連の処理が終了する。

【 0 0 8 8 】

以上の説明では、暗号鍵と暗号コンテンツの複製要求を行った場合の手順を述べたが、暗号鍵と暗号コンテンツの返却要求を行った場合の手順は、認証完了後に暗号鍵のみを消去することを除いては、実施の形態 1 の（２）と同様のため割愛する。

上記のように本発明の第 3 の実施の形態では、認証部を有するサーバおよび端末をネットワークで接続し、グループ内外の区別が可能となり、複製の範囲を有限なものにとどめる事で、情報の不正な複製の拡大を防止できる。

【 0 0 8 9 】

また、グループ内におけるユーザの私的利用を目的とした複製に関しても、これまでのコピープロテクション技術に比べ自由度が高く、ユーザの利便性を高めることができる。

また、データ量が大きい暗号化コンテンツを、可能な限り通信時間の短いグループ内端末よりダウンロードし、暗号鍵のみをグループ内サーバに取りに行くため、コンテンツのダウンロード時間を短く保ちつつ、厳密に使用可能なコンテンツの複製数を管理することができる。

【 0 0 9 0 】

なお、以上の説明では、暗号化コンテンツのダウンロード元を、最も応答が早い端末としたが、予め配布されている端末の処理性能データと、応答してきた端末のリストを照合し、最も処理性能が高い端末を選択しても構わないし、本システムの管理者が予め設定した端末の優先度と、応答してきた端末のリストを照合

し、最も優先度が高い端末を選択しても構わない。

（実施の形態 4）

本発明の実施の形態 4 に係る情報複製管理システムを図 1 5 を用いて説明する。

【 0 0 9 1 】

本情報複製管理システムの場合も、実施の形態 1 で説明したグループ 1 0 2 の概念が同様に存在するものとする。

情報複製管理システムの構成は、実施の形態 3 と同様である。

ここで、本実施の形態の全端末には、実施の形態 1 でその役割を述べた複製制限情報管理部 1 5 0 1、1 5 0 4 と、実施の形態 3 でその役割を述べたコンテンツ配布元決定部 1 3 0 3、1 3 3 0 を有す。

【 0 0 9 2 】

本実施の形態では、実施の形態 1 で説明したコンテンツの複製時に、複製制限情報も同時にダウンロードするものとする。その際に、ダウンロードする複製制限情報内のグループ内複製数は、ダウンロード元の複製制限情報管理部内のグループ内複製数を N （ N は整数）とすると、それを以下の値 M （ M は整数）に設定できる。それに伴い、ダウンロード元の複製制限情報管理部内のグループ内複製数は $N - M$ になる。以上の説明は、コンテンツを複製する場合を述べたが、その逆のコンテンツを返却する場合には、返却先のグループ内複製数が、現在の値と返却された複製制限情報内のグループ内複製数の和になる。

【 0 0 9 3 】

まず、以下でグループ内端末 1 1 0 5 がコンテンツの複製要求を行った場合の手順を説明する。なお、説明内では、既に上記のコンテンツ複製が行われ、複製数のグループ内端末に、コンテンツの複製があるものとして、話を進める。

まず最初に、コンテンツ配布元決定部 1 3 0 3 はグループに属している全ての端末に対し、所望のコンテンツを持っているかを確認する同報通信を通信部 2 2 3 を介して行う。その後、コンテンツ配布元決定部 1 3 0 3 は、最も早く応答したコンテンツを持っている端末を特定する。

【 0 0 9 4 】

そして、特定した端末に対して、コンテンツの複製要求を行う。ここで、この複製要求には、獲得したいグループ内複製数Mが含まれている。

それ以降の処理は、ダウンロードする内容がコンテンツと複製制限情報であることと、複製処理完了後のダウンロード元のグループ内複製数が「M」だけ差し引かれることを除いては、実施の形態1の(1)と同様である。

次に、グループ内端末1 1 0 5がコンテンツの返却要求を行った場合の手順を説明する。

【 0 0 9 5 】

まず最初に、本実施の形態におけるコンテンツの複製の場合と同様に、コンテンツ配布元決定部1 3 0 3は、最も早く応答したコンテンツを持っている端末を特定する。

そして、特定した端末に対して、コンテンツの返却要求を行う。ここで、この返却要求には、返却するグループ内複製数Mが含まれている。

【 0 0 9 6 】

それ以降の処理は、返却処理完了後の返却元のグループ内複製数に「M」が足されることを除いては、実施の形態1の(2)と同様である。

上記のように本発明の第4の実施の形態では、認証部を有するサーバおよび端末をネットワークで接続し、グループ内外の区別が可能となり、複製の範囲を有限なものにとどめる事で、情報の不正な複製の拡大を防止できる。

【 0 0 9 7 】

また、グループ内におけるユーザの私的利用を目的とした複製に関しても、これまでのコピープロテクション技術に比べ自由度が高く、ユーザの利便性を高めることができる。

また、コンテンツを可能な限り通信時間の短いグループ内端末よりダウンロードするため、コンテンツのダウンロード時間を短く保ちつつ、厳密に使用可能なコンテンツの複製数を管理することができる。

【 0 0 9 8 】

更に、コンテンツと複製制限情報を複数の端末に保管することにより、故障が発生した場合のコンテンツと複製制限情報の全数消失を防ぐことが可能となる。

それに加え、コンテンツの複製を提供する端末が、グループ内サーバに集中せず、グループ内の処理負荷分散が可能となる。

なお、以上の説明では言及しなかったが、グループ内サーバがコンテンツの複製経路や、各端末のグループ内複製数を管理しても構わない。

(実施の形態 5)

本発明の実施の形態 5 に係る情報複製管理システムを図 1 5 を用いて説明する。

【0099】

情報複製管理システムの構成は、実施の形態 4 と同様である。

先に説明した本実施の形態 1 では、グループ内サーバ 1 0 4 のみがコンテンツの複製制限情報を保管しているおり、もしグループ内サーバ 1 0 4 が故障し、複製制限情報が消失した場合、それ以降コンテンツの複製が不可能となる課題を有する。

【0100】

そこで、本実施の形態では、その課題を解決するために、コンテンツの複製制限情報をグループ内サーバ 1 0 4 以外のグループ内端末にバックアップしておく。そして、もしグループ内サーバ 1 0 4 が故障した場合に、そのバックアップデータを新たに設置したグループ内サーバに転送することで、コンテンツの複製が再開できるようにする。

【0101】

以下では、コンテンツの複製制限情報のバックアップ手順を、実施の形態 1 の(1)および(2)で説明した処理に追加する。なお、本説明では複製制限情報のバックアップデータを、グループ内端末 1 1 0 5 に保管するものとする。また、グループ内端末 1 1 0 5 は、複製制限情報のバックアップを保管する役目を開始する前に、グループ内サーバ内の全ての複製制限情報を、自己の複製制限情報管理部にコピーするものとする。

【0102】

まず最初に、実施の形態1の(1)および(2)の処理で、複製制限情報排他制御部207内のキューより先頭の処理要求を取り除く直前、つまりグループ内サーバ104内で複製制限情報が更新直後のタイミングで、更新された複製制限情報のみを特定する。次に、特定した複製制限情報を、通信部203を介してグループ内端末1105に送信し、グループ内端末1105は受信した複製制限情報を複製制限情報管理部1501に転送し、複製制限情報管理部1501は送られてきた複製制限情報の格納場所を特定した後、その複製制限情報を特定した格納場所に保管する。以上の処理が完了すると、グループ内端末1105はバックアップ完了通知をグループ内サーバ104に通信部223を介して送信し、グループ内サーバ104はバックアップ完了通知を受け取り次第、複製制限情報排他制御部207内のキューより先頭の処理要求を取り除く。以上で、複製制限情報のバックアップ処理が終了する。

上記のように本発明の第5の実施の形態では、グループ内サーバ104が故障し、複製制限情報が消失した場合でも、他のグループ内端末に複製制限情報のバックアップが存在するため、そのバックアップデータを新たに設置したグループ内サーバに転送することで、コンテンツの複製が再開できる。

【0103】

なお、以上の説明では、複製制限情報が更新されるたびに、バックアップを行っていたが、ある一定間隔ごとに複製制限情報のバックアップを行っても構わない。

また、以上の説明では、更新された複製制限情報のみをバックアップしていたが、その他の単位で複製制限情報をバックアップしても構わない。

(実施の形態6)

本発明の実施の形態6に係る情報複製管理システムを図16を用いて説明する。

【0104】

本実施の形態で使用する端末には、新たに複製したコンテンツの使用可能期間を管理する使用可能期間管理部を有し、

この使用可能期間管理部は、コンテンツの複製時に添付される使用可能期間情報を用いて、コンテンツの複製先は使用可能期間の終了時に、コンテンツを自動的に消去する。また、コンテンツの複製元の使用可能期間管理部は、当該コンテンツのグループ内複製数を「1」だけ増加させる。

【0105】

以下では、コンテンツの使用可能期間を制御するための手順を説明する。

まず最初に、グループ内サーバ104からグループ内端末1105へコンテンツをダウンロードする手順は、実施の形態1で説明したものと同様である。ただし、グループ内サーバ104はコンテンツの送信時に、そのコンテンツの使用可能期間情報を使用可能期間管理部1601に登録する。そして、コンテンツとともに登録した使用可能期間情報もグループ内端末1105に送る。グループ内端末1105は、ダウンロードされた使用可能期間情報1604を使用可能期間管理部1603に格納する。

【0106】

各使用可能期間管理部は、その内部の計時機能を使用し、使用可能期間情報に記載されたコンテンツ使用可能終了時間の到来を待つ。その後に、コンテンツ使用可能終了時間が到来した場合には、グループ内サーバ104内の使用可能期間管理部1601は、その旨を複製制限情報管理部204に通知し、グループ内複製数を「1」だけ増加させる。一方、グループ内端末1105の使用可能期間管理部1603は、使用可能期間が終了したコンテンツを記憶部211より削除する。以上で一連の処理が終了する。

上記のように本発明の第6の実施の形態では、時間に基づいた複製数の管理可能である。

【0107】

なお、以上の説明では、使用可能期間の終了時に、配布元では自動的に複製数を「1」だけ増加し、配布先では自動的にコンテンツを消去したが、配布先が配

布元に複製情報の返却要求を出し、通常どおりコンテンツを返却しても構わない。

また、配布先がリムーバブルメディアの場合には、使用可能期間の終了時に、グループ内サーバまたは端末に接続されていない場合があるため、その様な場合には使用可能期間の終了時以後、初めて接続された場合に、情報を消去するように実装しても構わない。

(実施の形態7)

本発明の実施の形態7に係る情報複製管理システムを図17を用いて説明する。

【0108】

本実施の形態で使用する端末には、新たに予め決定した時間にコンテンツの複製または返却を開始するための予約処理情報を管理する予約処理管理部を有し、

予約処理管理部は、複製もしくは返却の指示、およびその開始時間を予め設定した前記予約処理情報を用いて、前記開始時間の到来を期に、コンテンツの複製もしくは返却を開始させる。

【0109】

以下では、グループ内端末1105がコンテンツを予約複製する手順を説明する。

まず最初に、グループ内端末1105は、事前に複製の指示とその開始時間を予約処理情報1704を作成し、予約処理管理部1703に格納する。

予約処理管理部1703は、その内部の計時機能を使用し、予約処理情報に記されたコンテンツの複製開始時間の到来を待つ。その後、コンテンツの複製開始時間が到来した場合には、グループ内端末1105は本実施の形態1の(1)で説明したコンテンツの複製方法と同様の方法で、グループ内サーバ104より所望のコンテンツの複製をダウンロードする。以上で一連の処理を終了する。

【0110】

次に、グループ内端末1105がコンテンツを予約返却する場合の手順は、事前に設定する予約処理情報に返却の指示をすることと、返却開始時間が到来し

た場合の処理として、本実施の形態 1 の (2) で説明したコンテンツの返却方法と同様の方法を用いることを除けば、上記の予約複製の手順と同様のため割愛する。

上記のように本発明の第 7 の実施の形態では、更に予め決定した時間に情報を複製または返却するため、それに要する時間を待たずに、次の行動、例えばコンテンツ再生をすることが可能となる。

【0111】

なお、以上の説明では、コンテンツの予約複製情報をグループ内端末内にのみ格納したが、グループ内サーバにも予約複製情報を送付し、その時点でグループ内複製数が不足している場合には、予め他のグループ内端末からコンテンツを返却してもらい、複製開始時間に確実にコンテンツの複製ができるような実装をしても構わない。

【0112】

(その他の変形例)

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は、上記の実施の形態に限定されないのはもちろんである。以下のような場合も本発明に含まれる。

(1) 上記の各装置は、具体的には、マイクロプロセッサ、ROM、RAM、ハードディスクユニット、ディスプレイユニット、キーボード、マウスなどから構成されるコンピュータシステムである。前記 RAM 又は前記ハードディスクユニットには、コンピュータプログラムが記憶されている。前記マイクロプロセッサが、前記コンピュータプログラムに従って動作することにより、各装置は、その機能を達成する。

【0113】

(2) 本発明は、上記に示す方法であるとしてもよい。また、これらの方法をコンピュータにより実現するコンピュータプログラムであるとしてもよいし、前記コンピュータプログラムからなるデジタル信号であるとしてもよい。

また、本発明は、前記コンピュータプログラム又は前記デジタル信号をコンピ

ユーザ読み取り可能な記録媒体、例えば、フレキシブルディスク、ハードディスク、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD (Blu-ray Disc)、半導体メモリなど、に記録したものとしてもよい。また、これらの記録媒体に記録されている前記コンピュータプログラム又は前記デジタル信号であるとしてもよい。

【0114】

また、本発明は、前記コンピュータプログラム又は前記デジタル信号を、電気通信回線、無線又は有線通信回線、インターネットを代表とするネットワーク等を経由して伝送するものとしてもよい。

また、本発明は、マイクロプロセッサとメモリとを備えたコンピュータシステムであって、前記メモリは、上記コンピュータプログラムを記憶しており、前記マイクロプロセッサは、前記コンピュータプログラムに従って動作するとしてもよい。

【0115】

また、前記プログラム又は前記デジタル信号を前記記録媒体に記録して移送することにより、又は前記プログラム又は前記デジタル信号を前記ネットワーク等を経由して移送することにより、独立した他のコンピュータシステムにより実施するとしてもよい。

(3) 上記実施の形態及び上記変形例をそれぞれ組み合わせるとしてもよい。

【0116】

【発明の効果】

本発明は、著作権者の権利を保護しつつ、ユーザにとって利便性のあるシステムを提供する。具体的には、ユーザの私的利用を目的としたコンテンツの再生／複製等を許可する一方で、その複製数をネットワークを介して明確に制限して著作権者に対する権利の侵害を防止する効果を有する。

【図面の簡単な説明】

【図1】

本発明に係る情報複製管理システムの概略およびグループの概念を示すイメージ図。

【図 2】

グループ内サーバ、グループ内端末 1 およびグループ内端末 2 の内部構成と、各機器間のネットワーク接続形態を示す図。

【図 3】

本実施の形態 1 の (1) におけるグループ内情報複製処理を示すフローチャート。

【図 4】

本実施の形態 1 の (2) におけるグループ内情報返却処理を示すフローチャート。

【図 5】

グループ内サーバ、グループ外端末 1 の内部構成と、各機器間のネットワーク接続形態を示す図。

【図 6】

本実施の形態 1 の (3) におけるグループ外情報複製処理を示すフローチャート。

【図 7】

本発明に係る情報複製管理システム（着脱可能記憶媒体を含む）の概略およびグループの概念を示すイメージ図。

【図 8】

本実施の形態 2 の (1) および (2) における、グループ内サーバおよびグループ内着脱可能記憶媒体 1 の内部構成と、それらの接続形態を示す図。

【図 9】

本実施の形態 2 の (1) における、グループ内情報複製処理を示すフローチャート。

【図 10】

本実施の形態 2 の (2) における、グループ内情報返却処理を示すフローチャート。

【図 11】

本実施の形態 2 の (3) における、グループ内サーバ、グループ内端末 1 およ

びグループ内着脱可能記憶媒体 2 の内部構成と、それらの接続形態を示す図。

【図 1 2】

本実施の形態 2 の (3) における、グループ内情報返却処理を示すフローチャート。

【図 1 3】

本実施の形態 3 における、グループ内サーバ、グループ内端末 1 およびグループ内端末 2 の内部構成と、それらの接続形態を示す図。

【図 1 4】

本実施の形態 3 における、グループ内情報複製処理を示すフローチャート。

【図 1 5】

本実施の形態 4 における、グループ内サーバ、グループ内端末 1 およびグループ内端末 2 の内部構成と、それらの接続形態を示す図。

【図 1 6】

本実施の形態 6 における、グループ内サーバおよびグループ内端末 1 の内部構成と、それらの接続形態を示す図。

【図 1 7】

本実施の形態 7 における、グループ内サーバおよびグループ内端末 1 の内部構成と、それらの接続形態を示す図。

【符号の説明】

- 1 0 1 情報複製管理システム
- 1 0 2 グループ
- 1 0 3 ネットワーク
- 1 0 4 グループ内サーバ
- 1 0 5 グループ内端末 1
- 1 0 6 グループ内端末 2
- 1 0 7 グループ外端末 1
- 2 0 1、2 2 1 記憶部
- 2 0 2、2 2 2 認証部
- 2 0 3、2 2 3 通信部

2 0 4 複製制限情報管理部

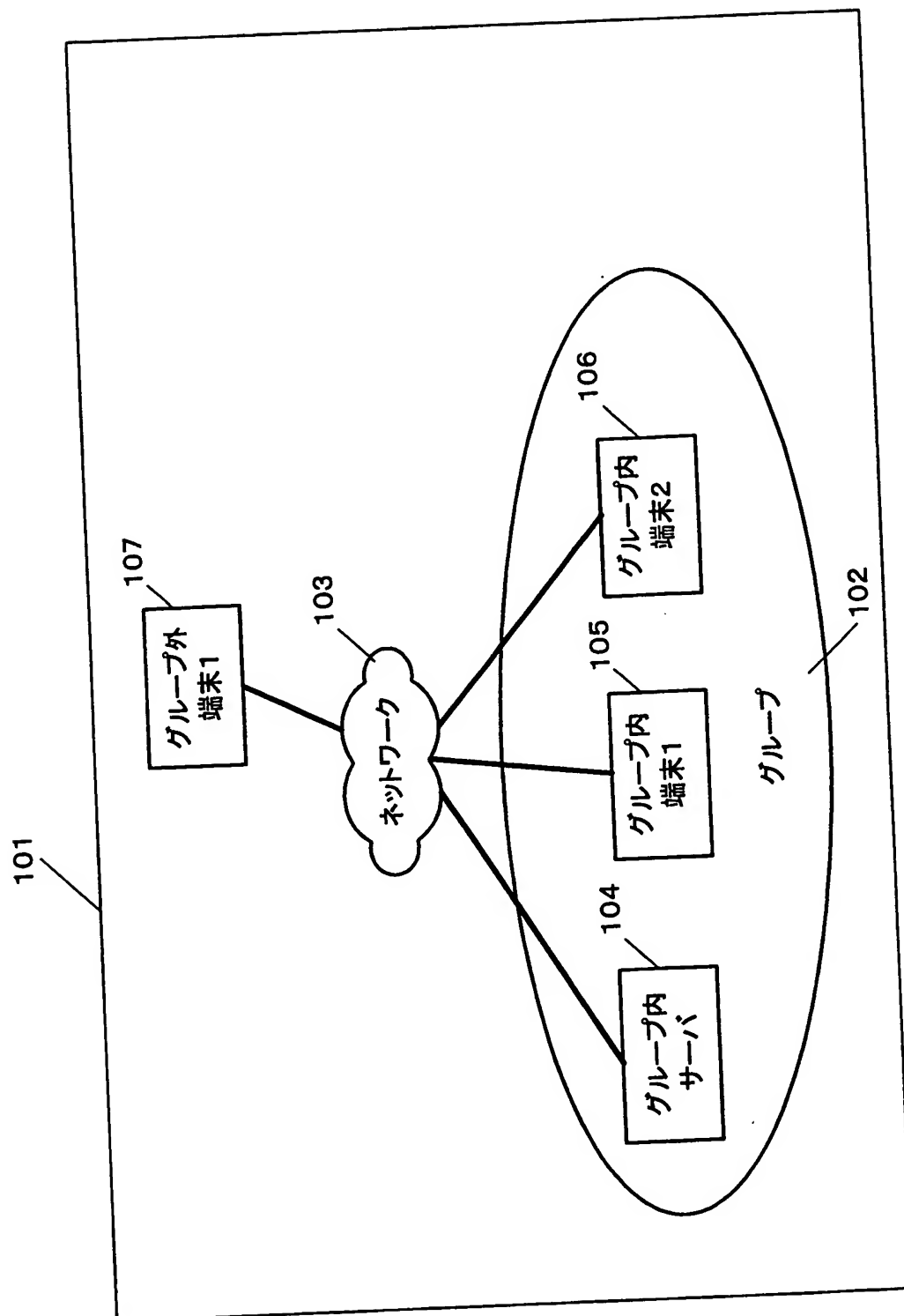
2 1 0 コンテンツ

2 1 1 グループ所属情報

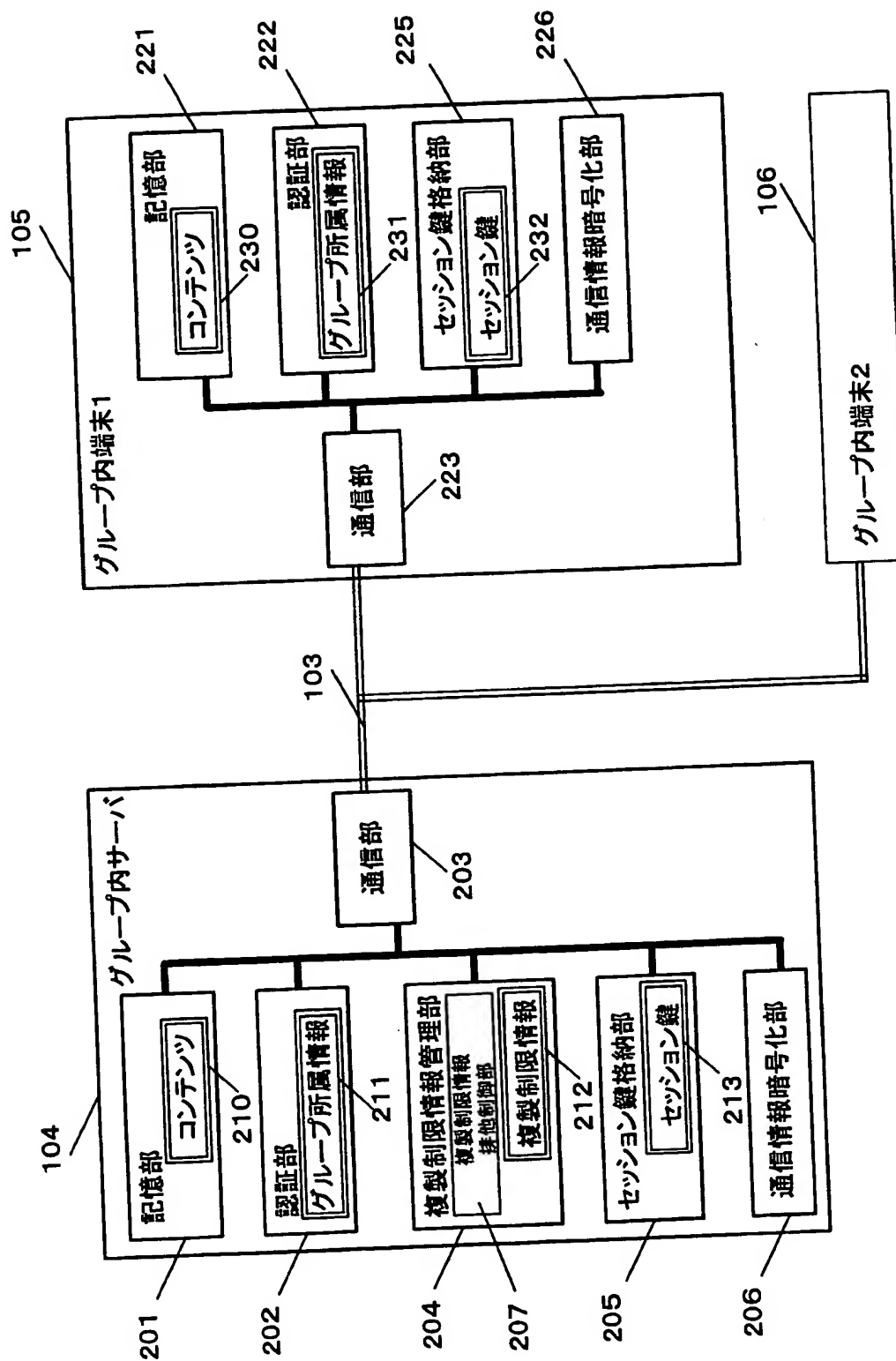
2 1 2 複製制限情報

【書類名】 図面

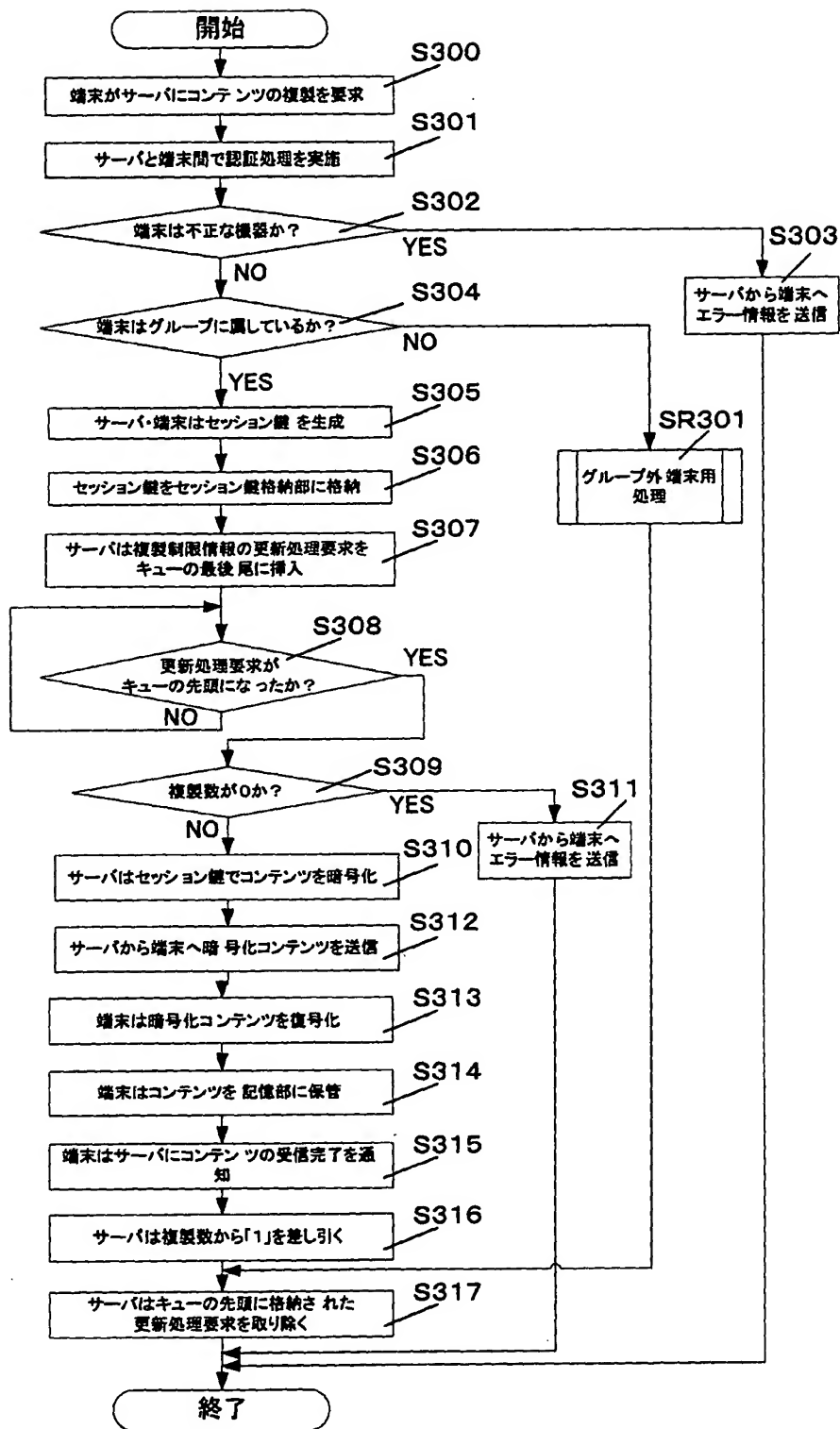
【図 1】



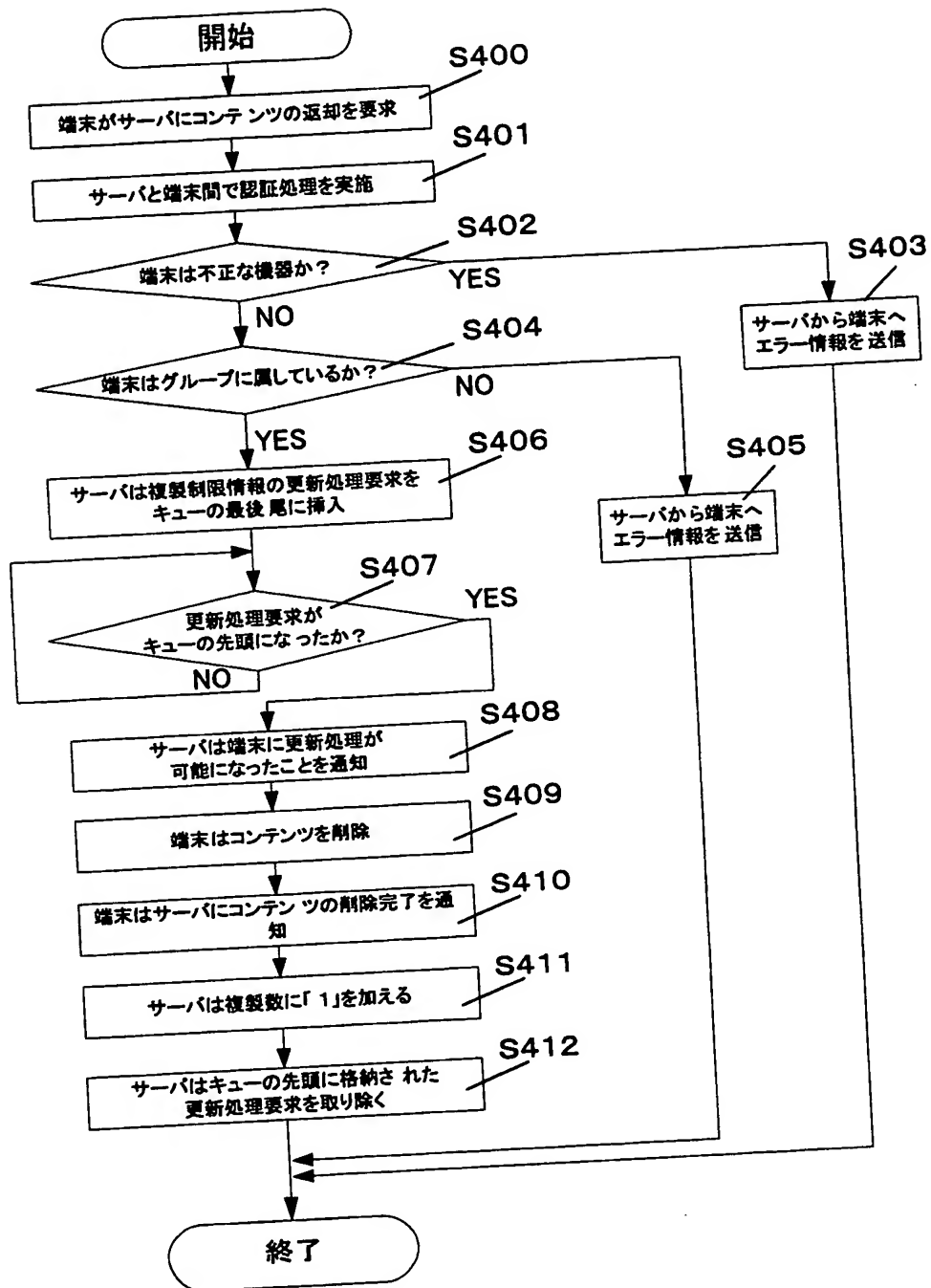
【図2】



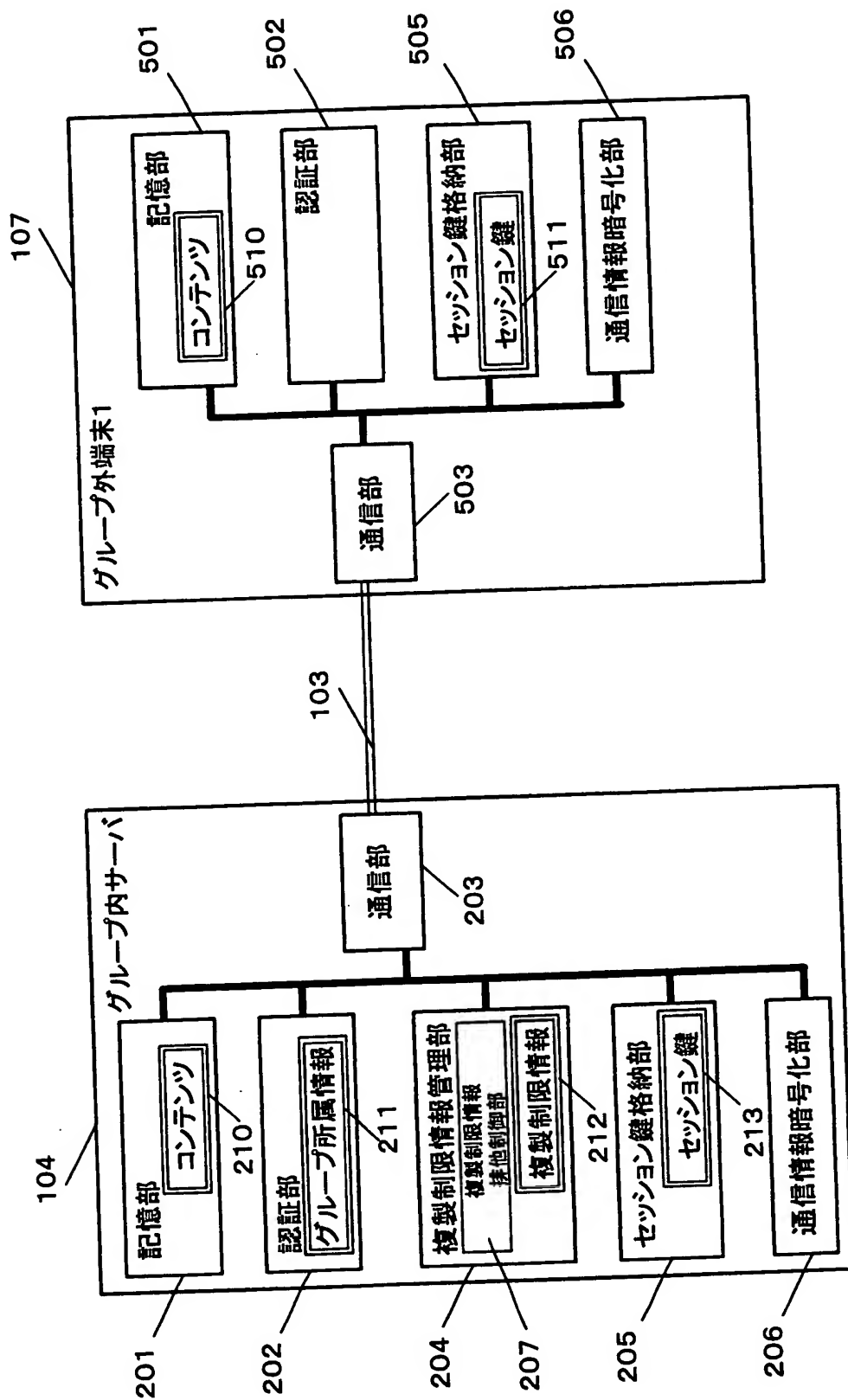
【図 3】



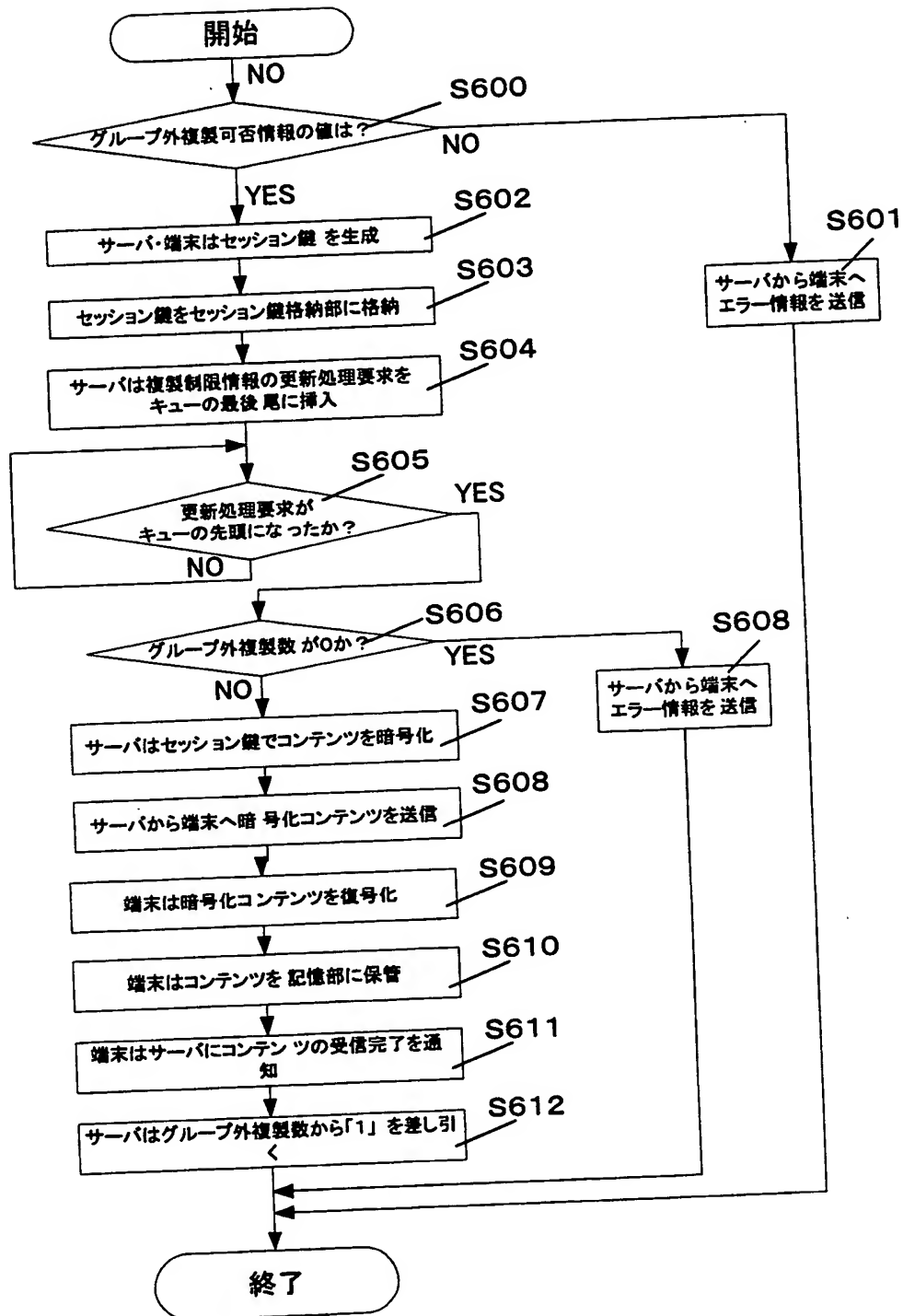
【図 4】



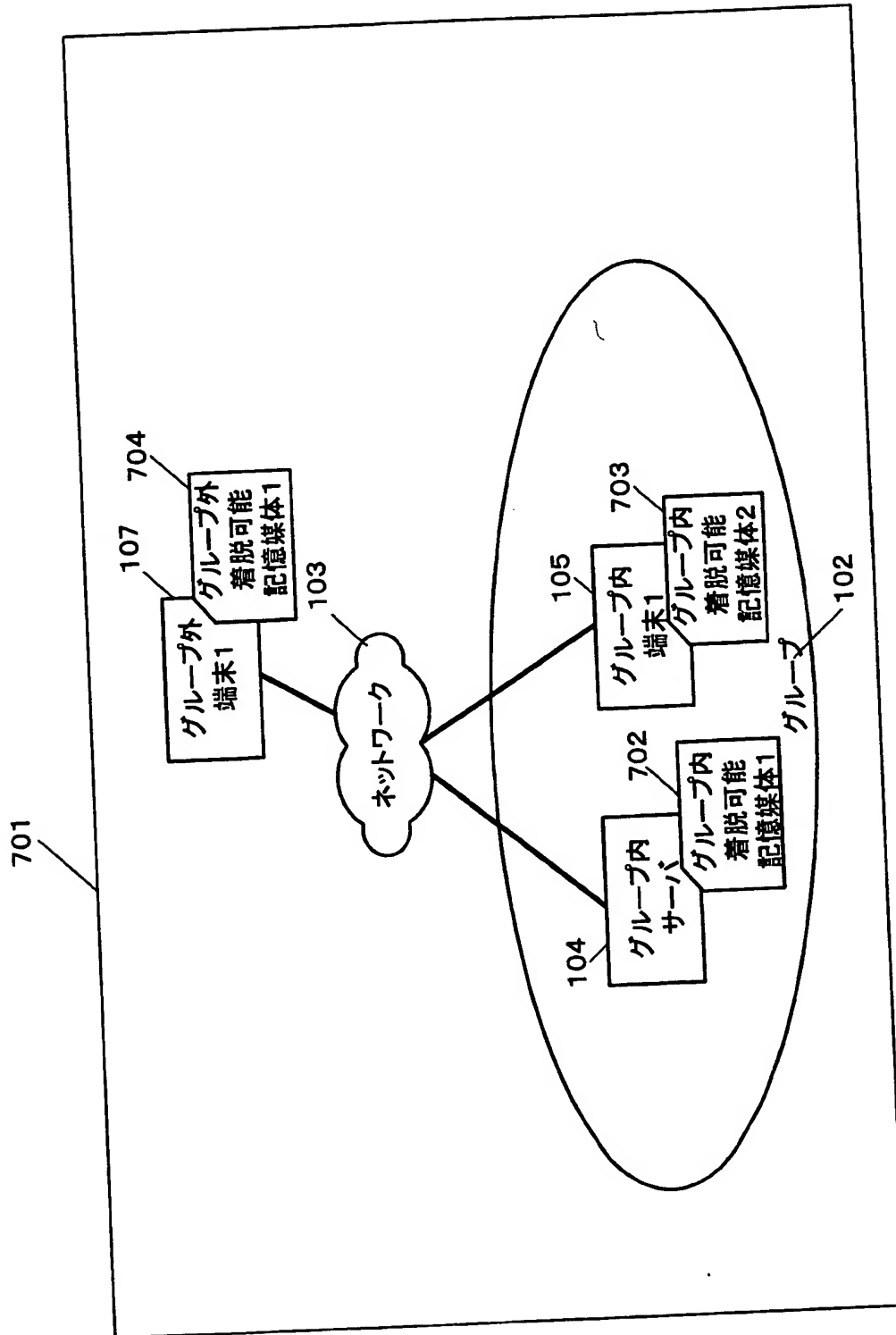
【図5】



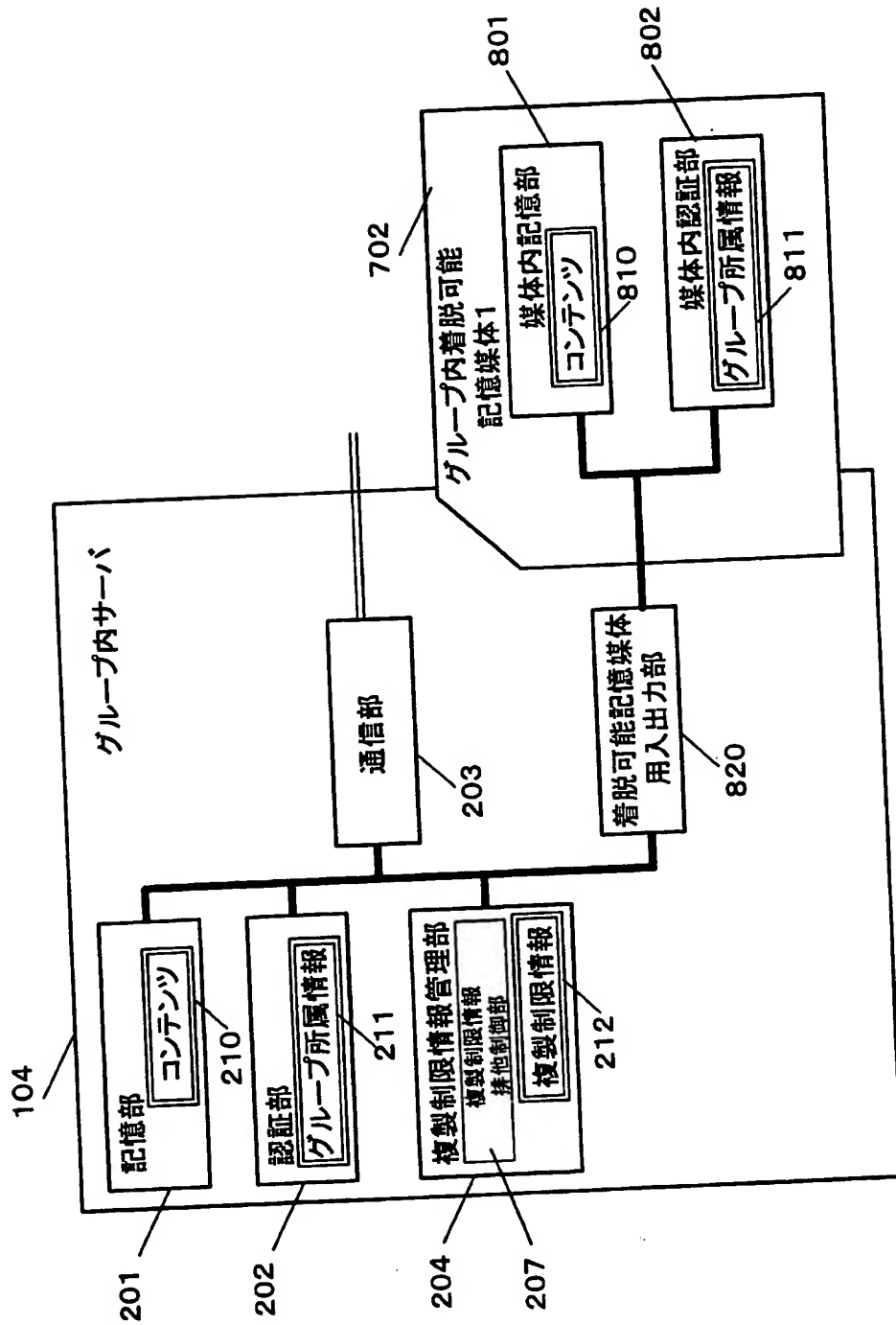
【図 6】



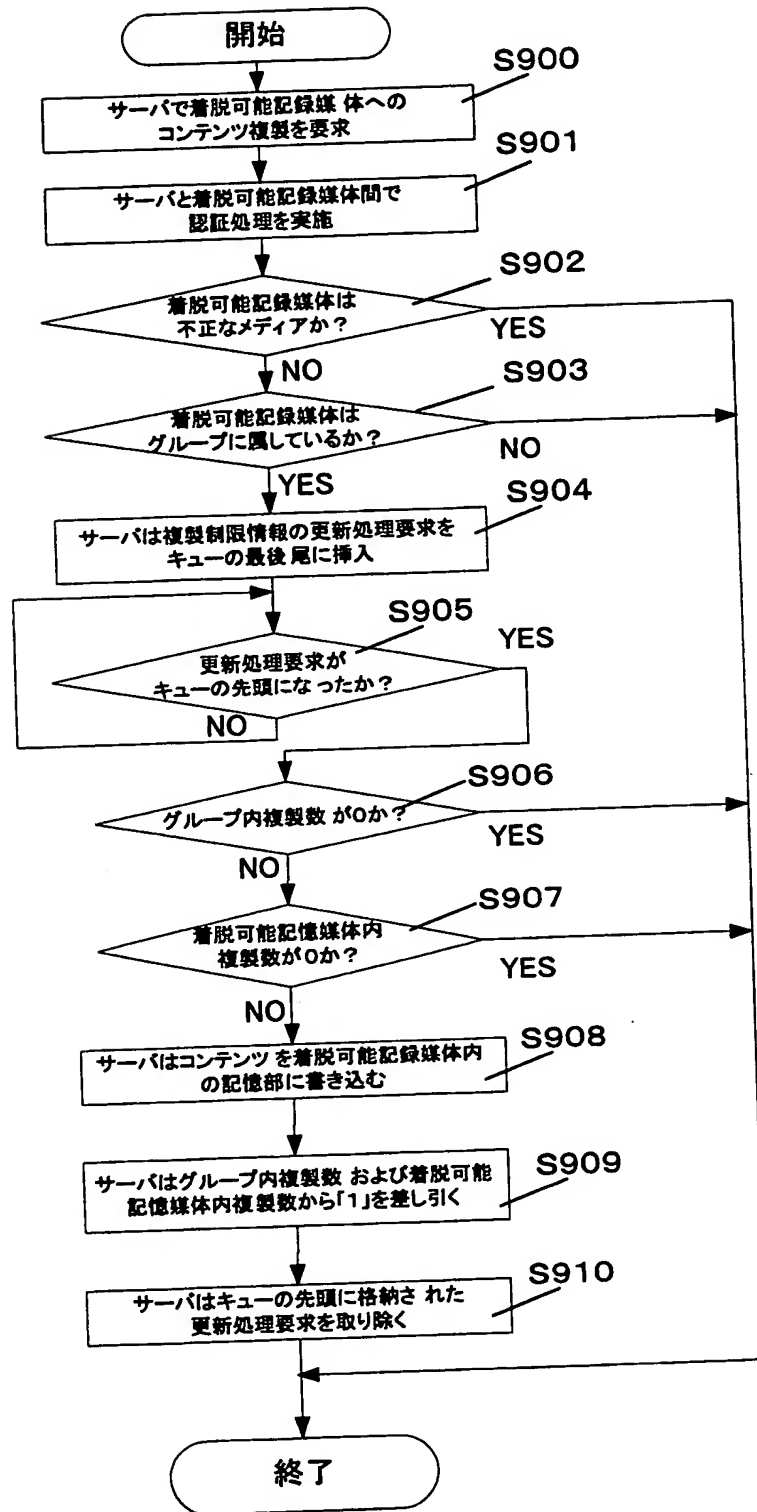
【図 7】



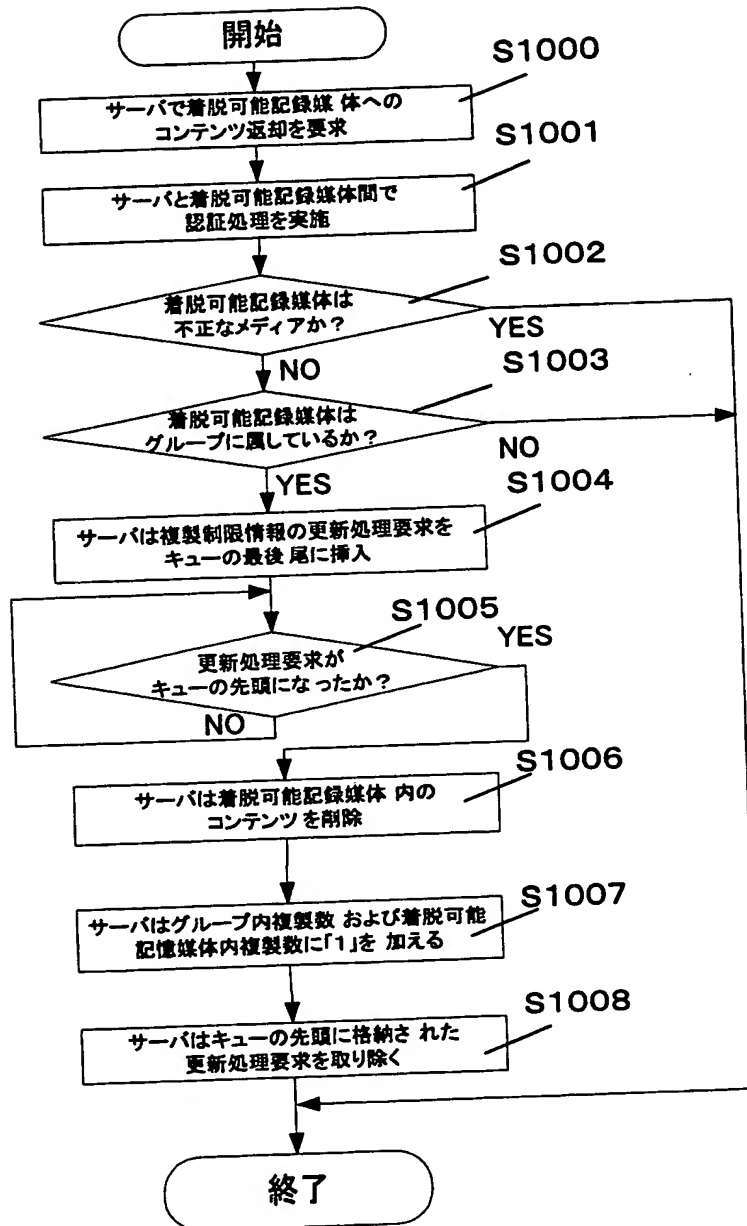
【図8】



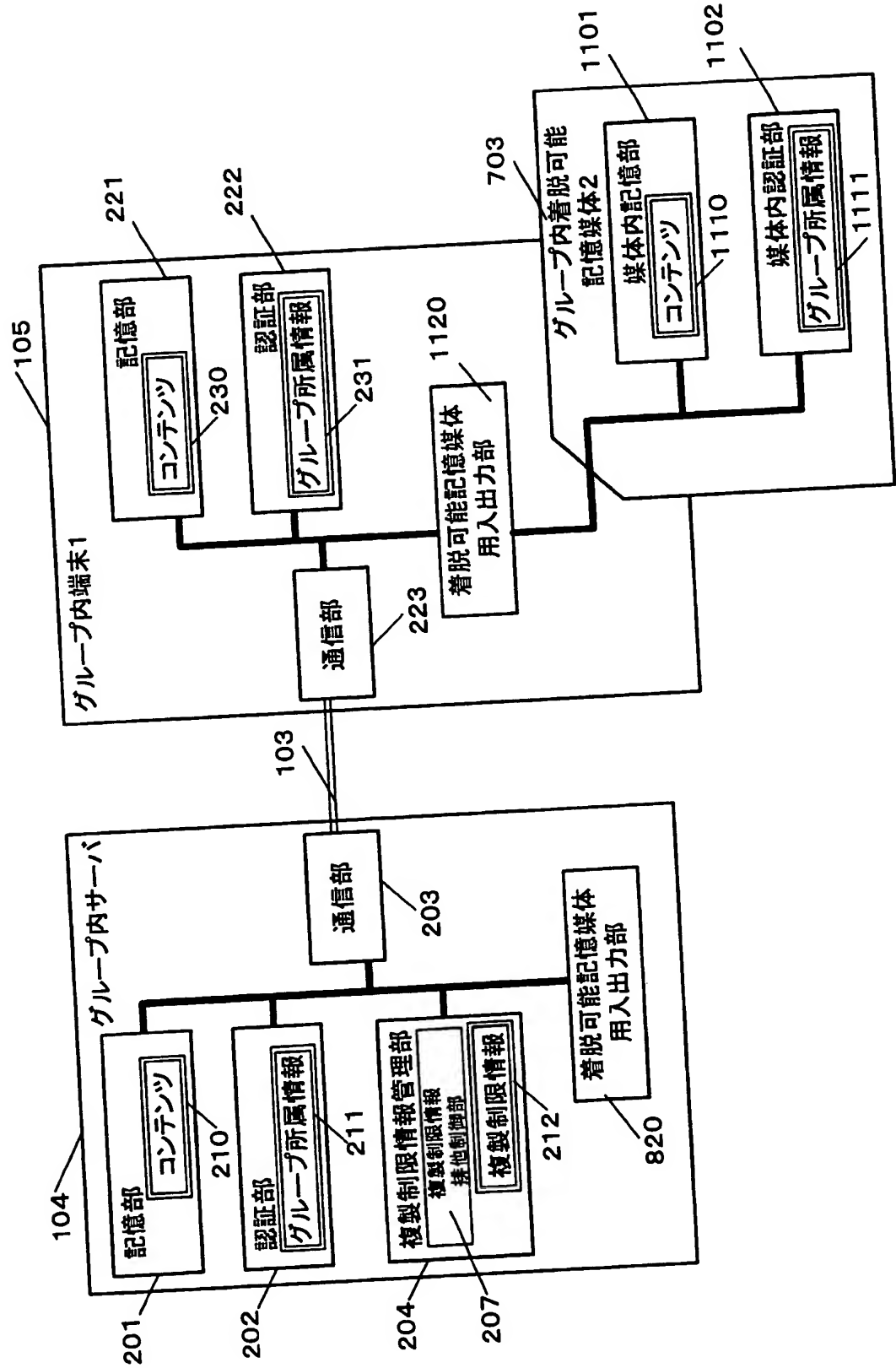
【図9】



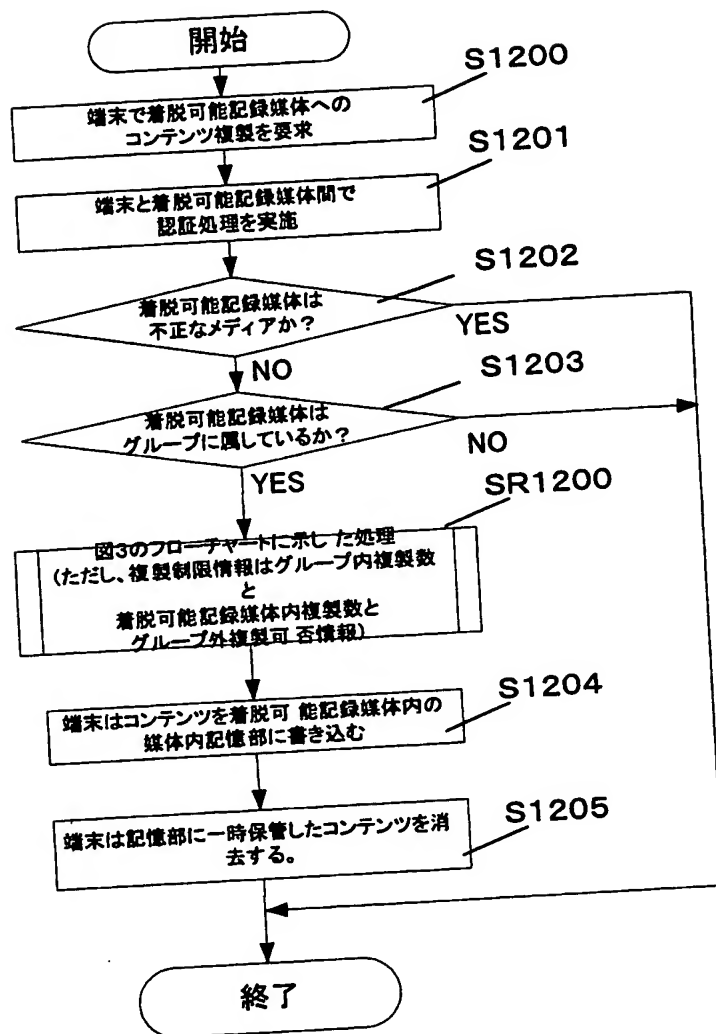
【図10】



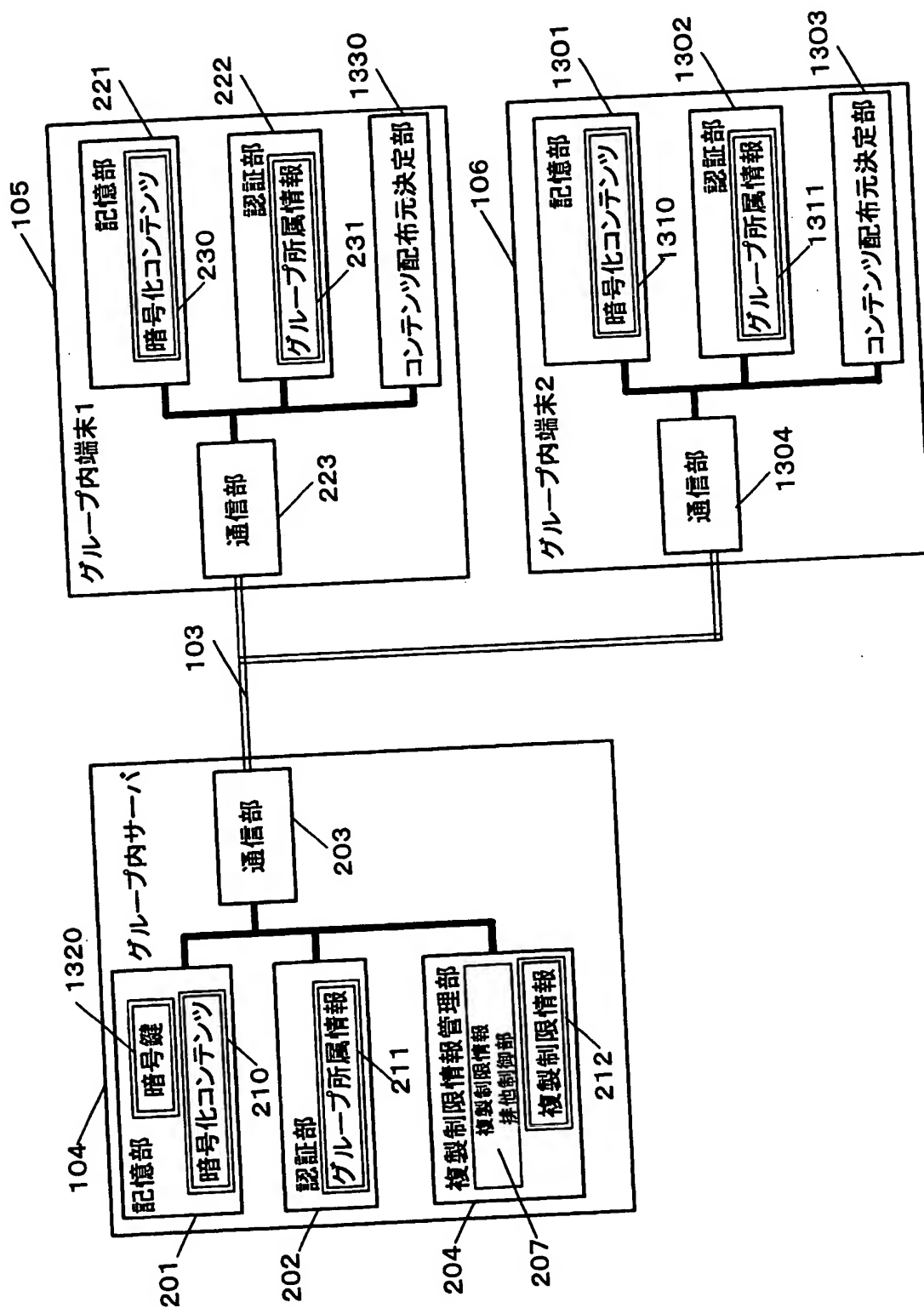
【図11】



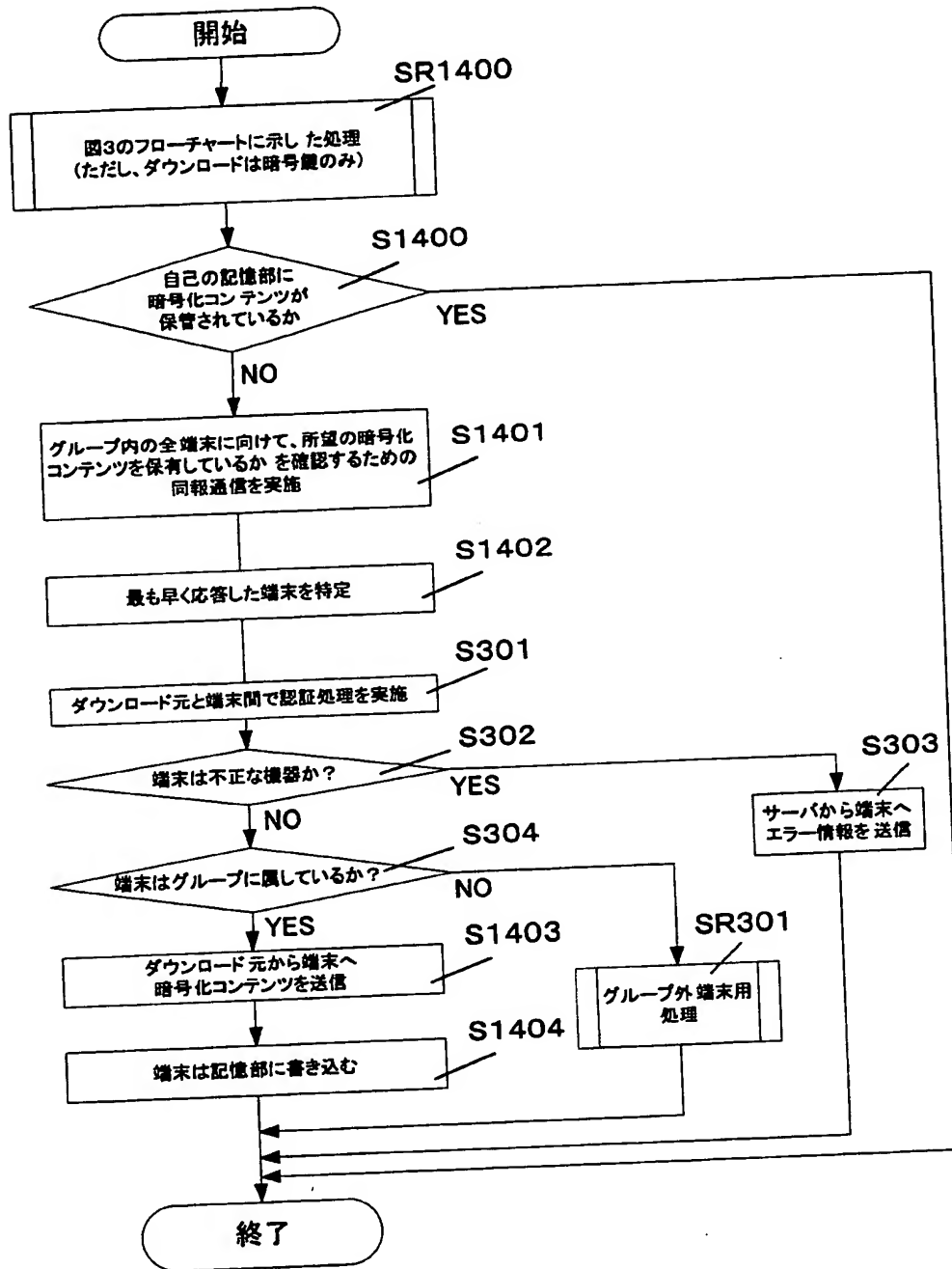
【図12】



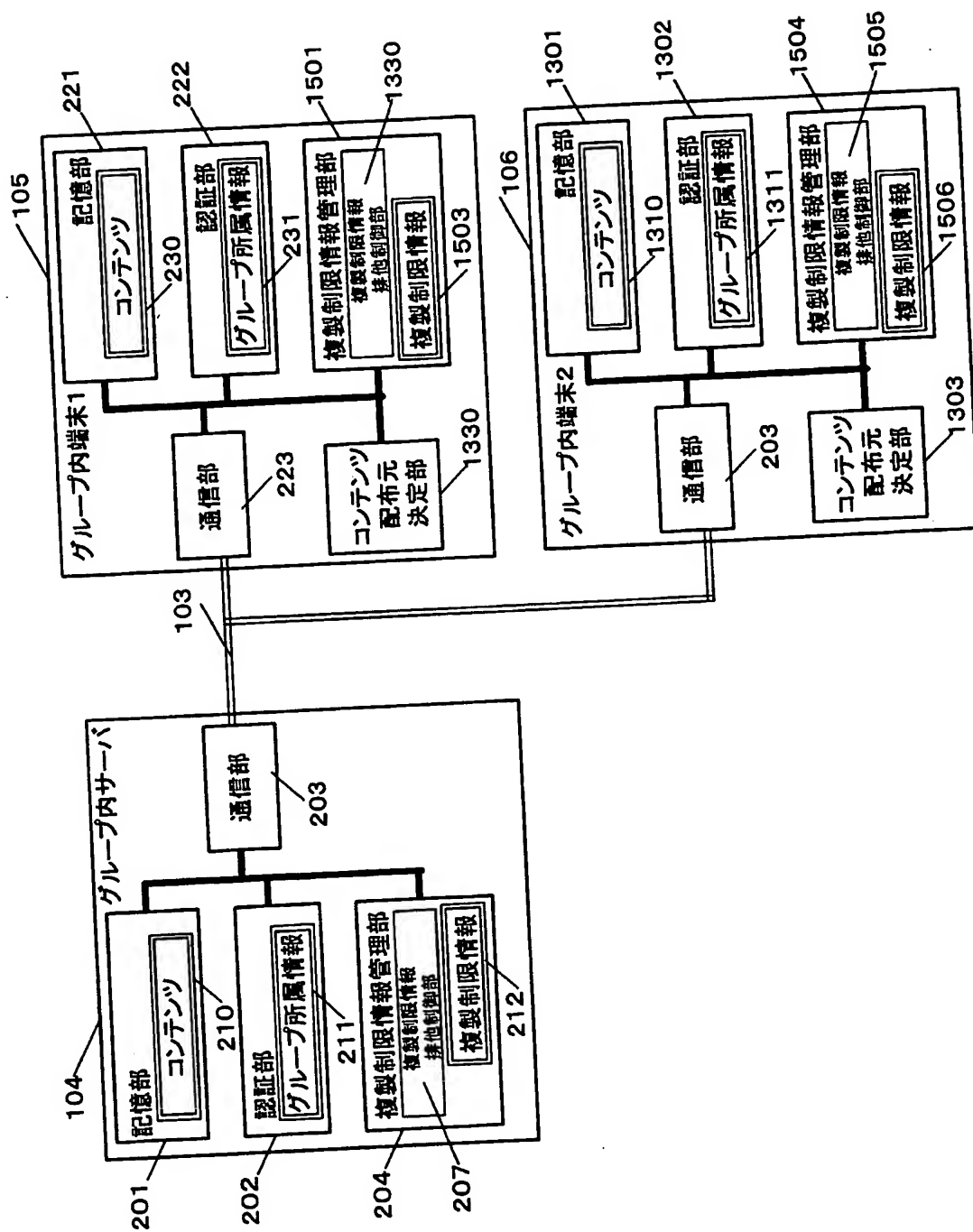
【図 13】



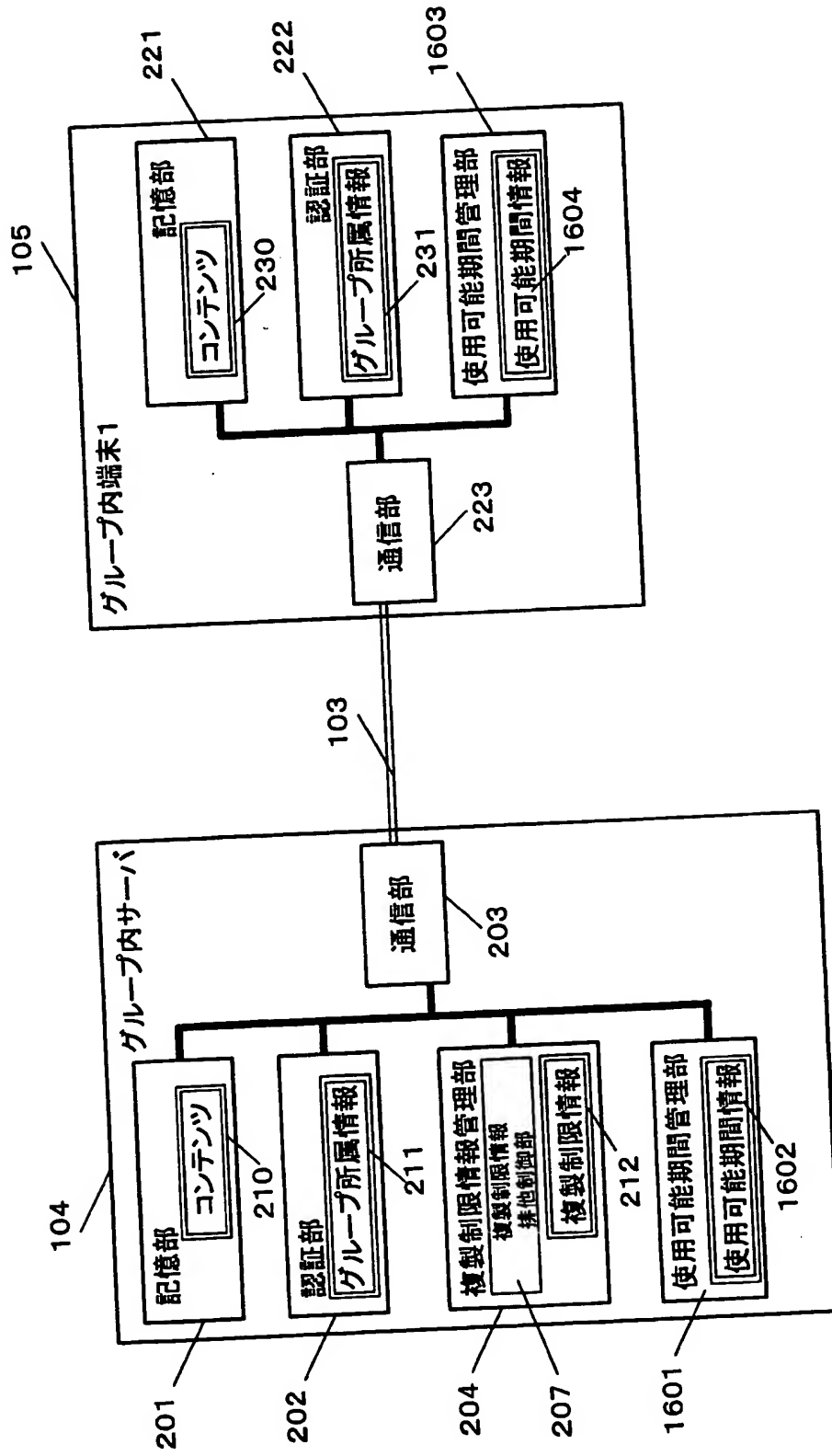
【図14】



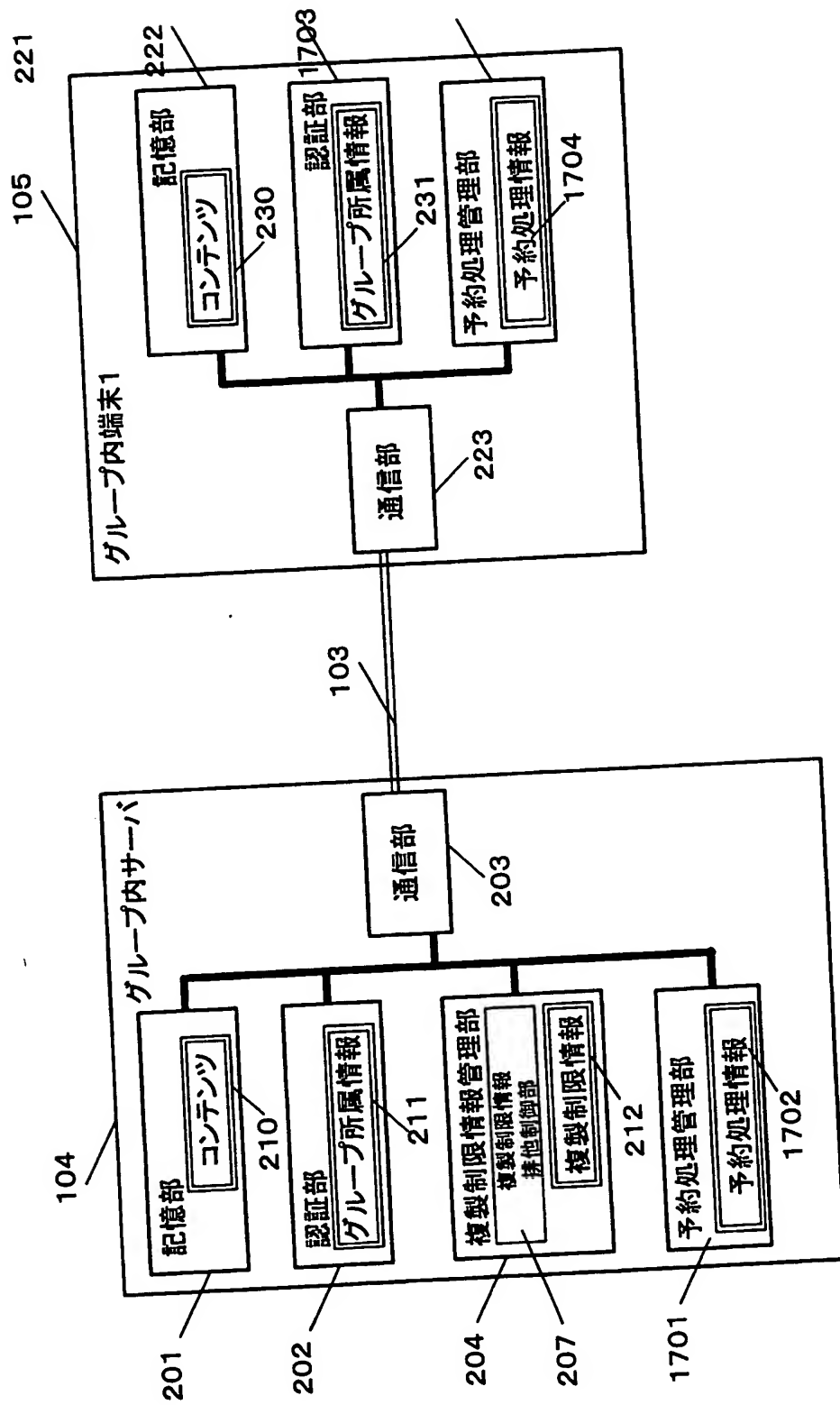
【図15】



【図16】



【図17】



【書類名】 要約書

【要約】

【課題】 ユーザの私的利用を目的としたコンテンツの複製等を許可し、利便性を高める一方で、その複製数を通信網を介して明確に制限して著作権者に対する権利の侵害を防止する。

【解決手段】 グループ属性を共有する複数の端末は、情報を格納するための記憶部と、他の端末と通信網を介して通信するための通信部と、他端末の正当性を確認するための認証部とを有し、第1の端末は、自らの記憶部または他端末内の記憶部に保管された情報のグループ内複製数を管理する複製制限情報管理部を有しており、複製制限情報管理部は、第2の端末から通信網を介して第1の端末に送付された情報複製要求、または複製情報の返却要求の正当性を認証部で確認した後に、当該情報の複製または返却の是非をグループ内複製数を基に判断し、複製または返却を許可した場合には当該情報のグループ内複製数を更新する。

【選択図】 図2

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社